Department of Defense
Enterprise Architecture Transition Strategy

Version 2.0
29 February 2008

Prepared by the DoD CIO Enterprise Architecture Congruence Community of Practice

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
29 FEB 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Department of Defense Enterprise Architecture Transition Strategy	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **DoD CIO Enterprise Architecture Congruence Community of Practice,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**98**	

Record of Changes from DoD EA Transition Strategy 28 Feb 2007

Change No.	Date of Change	Date Entered	Name of Person Entering Change
1. Changed version numbers and dates of relevant DoD documents	31 December 2007	31 December 2007	Marilee Cunningham, IDA
2. Added User's Guide Section	18 January 2008	18 January 2008	Marilee Cunningham, IDA
3. Updated Introduction and NCE Sections with changes from the 2007 version	31 December 2007	31 December 2007	Marilee Cunningham, IDA
4. Added relevant topics to Current Status Section, including expanded discussion of Net-Centric and other DoD Strategies	31 December 2007	31 December 2007	Marilee Cunningham, IDA
5. Updated Target Capability View section with GIG Architectural Vision content	31 December 2007	31 December 2007	Marilee Cunningham, IDA
6. Updated Transition Strategy Analysis section, using analysis of 65 DoD IT 300 Exhibit investments as the sample set	31 December 2007	31 December 2007	Marilee Cunningham, IDA
7. Deleted Remediation Section and moved content to Current Status section, and added Summary Section.	31 December 2007	31 December 2007	Marilee Cunningham, IDA

Table of Contents

Table of Figures

Users' Guide

The DoD Enterprise Architecture (EA) Transition Strategy 2008 follows the outline in the Federal Practice Guidance, November 2007, for developing a Transition Strategy and meeting the criteria for the OMB EA Assessment. To help the reader to understand the document, a description of the sections and their content follows:

- **Section 1. Introduction.** This section describes the purpose, intended audience, and approach to developing the DoD EA Transition Strategy.

- **Section 2. The DoD Net-Centric Enterprise.** This section addresses the Mission and Change Drivers of DoD and by outlining the Quadrennial Defense Review (QDR) goals for transformation and the inherent need for a transition strategy to track progress toward the future Net-Centric Environment (NCE).

- **Section 3**: **Current State.** This section describes the progress the Department has made architecting the complex Global Information Grid (GIG) and ongoing efforts. It includes the current status and summary content of the GIG Architecture; DoD strategies and policies; GIG Governance; Mission Area Segment Architectures; Internet Protocol v6; a cross-agency initiative summary; portfolio and capability management; and transition planning processes

- **Section 4: Target Capability View.** This section describes the GIG Architectural Vision, the vision for the DoD "target" architecture for the Net-Centric Environment (NCE). This is updated from the GIG Capstone description in the DoD EA Transition Strategy 2007.

- **Section 5: DoD EA Transition Strategy Analysis Concept and Components.** This section .includes the what, why, and how as well as the elements of the DoD EA Transition Strategy.

- **Section 6: DoD EA Transition Strategy Analysis.** This section includes an analysis of Mini-Transition Strategies, Net-Centric Maturity Models, and performance information. The 65 DoD Component IT300 initiatives were used as a sample set to represent DoD transition planning.

- **Section 7: DoD EA Transition Strategy Summary.** This section restates the outline of the document, ties together the sections, and presents the overall picture that the DoD EA Transition Strategy is intended to convey.

Section 1. Introduction

This section describes the purpose, intended audience, and approach to developing the DoD EA Transition Strategy.

Section 1 Contents:

Purpose of the Department of Defense (DoD) Enterprise Architecture (EA) Transition Strategy

The DoD EA Transition Strategy serves as the foundation to modernize and transform activities by describing DoD's plan to migrate from its 'baseline' architecture as described in the federated GIG architecture to its 'target' architecture as outlined in the GIG Architectural Vision, by defining projects, programs, timelines and milestones in the context of transition and sequencing plans. Development of a DoD EA Transition Strategy is mandated by the Office of Management and Budget (OMB) guidance which takes its authority from OMB Circular A-11, IT.300 Exhibits, OMB Circular A-130; Government Performance and Results Act (GPRA); the Clinger-Cohen Act, and the E-Government Act and good management practice.

Intended Audience

The primary audience for the DoD EA Transition Strategy includes DoD executives and managers at all levels to include portfolio managers, strategic planners, resources planners, strategic enterprise architects, internal organizations with cross-DoD capability relationships, external organizations with cross-agency relationships with DoD programs and projects, including OMB and the Government Accounting Office (GAO).

Approach to Development of the DoD EA Transition Strategy

Transformation is not only a goal for the Department of Defense to become more effective and efficient but it also connotes the continuous process improvement that does not end with a set of specific accomplishments.

The approach to development of the DoD EA Transition Strategy is to:

- educate and maintain currency of DoD community with regard to all aspects (policies, strategies, definition, etc) of EA;
- document required as-is, to-be, and associated transition strategies;
- require and monitor performance metrics;

- utilize periodic analyses of the aforementioned to realize continuous process improvement and update of EA.

The DoD EA Transition Strategy is an annual report that describes and updates all DoD efforts toward this continuous improvement process. The basic content reflects the OMB criteria for a transition strategy as outlined in the *Federal Enterprise Architecture Practice Guidance*, November 2007, and the DoD version, *A Practical Guide for Bringing Enterprise Architecture Value to the Mission*, May 2007. In addition, OMB, through the OMB EA Assessment Framework, requires a transition strategy as a part of the DoD EA.

Because of the large and complex Department of Defense with its multiple missions, the DoD EA Transition Strategy encompasses a federated approach to its development. For example, the Business Transformation Agency (BTA) 2007 Enterprise Transition Plan (ETP) focuses specifically on the Business MA (BMA) and meets the criteria for an agency transition plan. The Enterprise Information Environment Mission Area (EIE MA) will publish an EA in January 2008 and plans to develop a Segment Architecture and Transition Strategy derived from the EA. The Warfighting MA (WMA), Defense Intelligence MA (DIMA), and Intelligence MA (IMA) are also in the process of developing EAs and their related segment architectures and transition strategies. Projected completion for the WMA and DIMA EAs is in late FY 2008/early FY 2009.

Internet Protocol v6 (IPv6), has also developed a transition strategy, the *IPv6 Transition Plan V2.0*, June 2006. In addition, as a sample set to exemplify DoD Components' transition planning, the 65 current Exhibit 300 investments have submitted Mini-Transition Strategies to be used as a basis for analysis in this DoD EA Transition Strategy,

Using the DoD EA Annual Plan (embedded in Appendix A), a plan for that addresses EA progress as a guide, the DoD EA Transition Strategy accomplishes the following:

- Provides a repeatable process for creating, maintaining, and managing the DoD EA Transition Strategy, including processes for performing gap analysis, alternatives analysis, and the management of projects over time.
- Provides a mechanism for identifying opportunities for consolidation or reuse and gaps between the "baseline" and "target" architecture.
- Documents defined programs and projects and sequencing plans in support of its target architecture.
- Addresses priorities and performance objectives identified in the 2006 QDR.
- Includes initiatives with milestones for at least one segment architecture, the Business EA (BEA) for DoD's Business Mission Area.
- Demonstrates clear linkage between Net-Centric capabilities in the Transition Strategy and investments in the DoD investment portfolio.

- Includes defined and measurable performance milestones that indicate the Department's success in achieving performance targets and has processes and tools in place to track performance.
- Identifies timelines for implementing net-centric attributes with supporting artifacts for investments in the IT300 Exhibit.

The approach for developing this DoD EA Transition Strategy to address the complex DoD environment and meet the criteria for the OMB EA Assessment Framework, includes the following steps:

- Describe associations with the DoD transformation goals from the 2006 QDR
- Describe the status of DoD EA as a federated baseline architecture and the status of ongoing transformation efforts
- Describe the GIG Architectural Vision and related artifacts that comprise the federated objective (target) architecture
- Analyze representative DoD IT300 Exhibit investments' transition strategies and their performance measures to document transformation progress. Summarize findings.
- Recommend an approach for continuous process improvement, including the DoD EA governance process and a DoD federated process that makes DoD Net-Centric transformation information visible, accessible, and understandable.

Section 2. DoD Net-Centric Environment (NCE)

This section addresses the Mission and Change Drivers of DoD and by outlining the Quadrennial Defense Review (QDR) goals for transformation and the inherent need for a transition strategy to track progress toward the future Net-Centric Environment (NCE).

Section 2 Contents:

- Description of the NCE

Description of the NCE

The DoD EA Transition Strategy links to the strategic goals of the Department as represented in the QDR 2006. These strategic goals cannot be accomplished without a strategy to transition from the existing environment represented by stove-piped systems and islands of information to the desired NCE, and a commitment to the changes necessary to accomplish the capabilities of the transformational NCE.

The DoD leadership envisions the NCE as the underpinning of the many changes foreseen in the QDR 2006, which is a top-down look at US defense strategy, taking into account the world environment, threats, current forces and programs, and the resources likely to be available. The Department foresees the need for continuous change, which builds on the ever changing world in which the warfighter operates. The QDR maps the way ahead for the next 20 years as the Department confronts current and future challenges and continues its transformation for the 21st century.

To characterize the nature of the Department's transformation, it should be viewed as a shift of emphasis to meet the new strategic environment. Examples of this shift in emphasis include:[1]

From a peacetime tempo	To a wartime sense of urgency
From a time of reasonable predictability	To an era of surprise and uncertainty
From single-focused threats	To multiple, complex challenges
From nation-state threats	To decentralized network threats from non-state enemies
From conducting war against nations	To conducting war in countries we are not at war with (safe havens)
From "one size fits all" deterrence	To tailored deterrence for rogue powers, terrorist networks and near-peer competitors
From responding after a crisis starts (reactive)	To preventive actions so problems do not become crises (proactive)
From crisis response	To shaping the future
From threat-based planning	To capabilities based planning

[1] 2006 Quadrennial Defense Review

From peacetime planning	To rapid adaptive planning
From a focus on kinetics	To a focus on effects
From 20th century processes	To 21st century integrated approaches
From static defense, garrison forces	To mobile, expeditionary operations
From under-resourced, standby forces (hollow units)	To fully-equipped and fully-manned forces (combat ready units)
From a battle-ready force (peace)	To battle hardened forces (war)
From large institutional forces (tail)	To more powerful operational capabilities (teeth).
From major conventional combat operations –	To multiple irregular, asymmetric operations
From separate military Service concepts of operation	To joint and combined operations
From forces that need to de-conflict	To integrated, interdependent forces
From exposed forces forward	To reaching back to CONUS to support expeditionary forces
From an emphasis on ships, guns, tanks and planes	To focus on information, knowledge and timely, actionable intelligence
From massing forces	To massing effects
From set-piece maneuver and mass	To agility and precision
From single Service acquisition systems	To joint portfolio management
From broad-based industrial mobilization	To targeted commercial solutions
From Service and agency intelligence	To truly Joint Information Operations Centers
From vertical structures and processes (stovepipes)	To more transparent, horizontal integration (matrix)
From moving the user to the data	To moving data to the user
From fragmented homeland assistance	To integrated homeland security
From static alliances	To dynamic partnerships
From predetermined force packages	To tailored, flexible forces
From the U.S. military performing tasks	To a focus on building partner capabilities
From static post-operations analysis	To dynamic diagnostics and real-time lessons learned
From focusing on inputs (effort)	To tracking outputs (results)
From Department of Defense solutions	To interagency approaches

This shift in emphasis depends on the changes enabled by the NCE. Harnessing the power of information connectivity defines Net-Centricity and serves as an underpinning of all other transformations. By enabling critical networked relationships between organizations and people, the Department will be able to accelerate the speed of business processes, operational decision-making and subsequent actions due to better, more timely information. The collection and dissemination of information should be managed by portfolios of capabilities that cut across legacy stove-piped systems. These capability portfolios require the identification of capability increments to measure

progress toward the NCE and to address gaps, redundancies, and opportunities for reuse.

The foundation for Net-Centric operations is the GIG, the target architecture described in the GIG Architectural Vision that includes a globally interconnected, end-to-end set of trusted and protected information networks. The GIG will enable the secure, agile, robust, dependable, interoperable data sharing environment for the Department where warfighter, business, and intelligence users share knowledge on a global network that facilitates information superiority, accelerates decision-making, effective operations, and Net-Centric transformation.

The Department has made steady progress implementing Net-Centric systems and concepts of operation. It has deployed an enhanced land-based network and new satellite constellation as part of the Transformational Communication Architecture (TCA) to provide high-bandwidth, survivable internet protocol communications. Together, they support battle-space awareness, time-sensitive targeting and communications capabilities on the move. Deployed terminals – from command and control (Joint Tactical Radio System) to very large bandwidth ISR systems – are extending the communications "backbone" down to the smallest tactical unit in the field.

Another foundation for Net-Centric operations is the DoD Net-Centric Data Strategy enabling the fusion of information from any platform or terminal. Pulling all this together, the revised Unified Command Plan has assigned U.S. STRATCOM lead responsibility to operate and protect the GIG. To move closer toward this vision and build on progress to date, the Department will:

- Strengthen its data strategy – including the development of common data lexicons, standards, organization, and categorization – to improve information sharing and information assurance, and extend it across a multitude of domains, ranging from intelligence to personnel systems.
- Increase investment to implement the GIG, defend and protect information and networks and focus research and development on its protection.
- Develop an information-sharing strategy to guide operations with Federal, state, local and coalition partners.
- Shift from Military Service-focused efforts toward a more Department-wide enterprise Net-Centric approach, including expansion of the Distributed Common Ground System.
- Restructure the Transformational Satellite (TSAT) program to "spiral develop" its capabilities and re-phase launches accordingly, and add resources to increase space-based relay capacity.
- Develop an integrated approach to ensure alignment in the phasing and pacing of terminals and space vehicles.
- Develop a new bandwidth requirements model to determine optimal network size and capability to best support operational forces.

Most of the Department's goals are enabled by this NCE and chances of them being realized are enhanced because of it. For example, DoD's efforts for fighting the long war against terrorism are enabled by the NCE because trusted relevant information is available to the war fighters as they carry out the mission of the enterprise. Similarly making operational the national defense and national military strategies depend on the NCE to make available ubiquitous high quality information that enhances decisions. Rapidly reorienting capabilities and forces depends on the ability to make better and faster decisions based on information about forces, capabilities, and threats. Without the new defense NCE, it would be next to impossible to reshape the defense enterprise and develop the total force ready and capable for achieving unity of effort in the 21st century.

However, any attempt to predict the future security environment of 2025 is inherently difficult. Given the dynamics of change over time, the Department must develop a mix of agile and flexible capabilities to mitigate uncertainty. The NCE directly contributes to this need. To meet the key challenges in this period, the department must: shape and sustain its Armed Forces to most effectively fight the War on Terrorism, transform "in stride" during wartime, strengthen our joint war fighting, and improve the quality of life of our Service members and their families.

Finally, it is important to note that the NCE is only one step of the continuum of transformation in the Department. Its purpose is to help shape the process of change to provide the United States of America with strong, sound and effective war fighting capabilities in the decades ahead. The QDR is the DoD's strategic plan that documents these ideas and provides a roadmap for the transformation from the legacy environment of today to the transformed Defense enterprise of tomorrow.

The DoD EA Transition Strategy is a reflection of these Net-Centric transformational goals of the QDR. Policies and guidance are in place or are being developed and/or reviewed to guide DoD executives and managers in the documentation and facilitate implementation of the Net-Centric transformation capabilities. Section 6 of this document outlines in more detail recommendations to evolve the process for the DoD EA Transition Strategy to all DoD programs in an incremental and federated manner.

Section 3. Current State

This section describes the progress the Department has made architecting the complex Global Information Grid (GIG) and ongoing efforts. It includes the current status and summary content of the GIG Architecture; DoD strategies and policies; GIG Governance; Mission Area Segment Architectures; Internet Protocol v6; a cross-agency initiative summary; portfolio and capability management; and transition planning processes

Section 3 Contents:

- Summary

Introduction

Net-Centric transformation is key to the DoD defense strategy to meet the challenges of the dangerous and uncertain security environment of the 21st Century. There are many initiatives in the Department of Defense that are in the planning stage or being implemented to transform how the military fights and how the Department does business. To set the stage for transformation, it is important to know the current status of DoD in regard to the "as-is" or federated baseline of the DoD EA as well as the progress made by the Department since the publication of the GIG Architecture and during calendar year 2007.

The content of each part and sub-part of this section comprises the overall DoD approach to transformation through the use of architecture, net-centricity, and portfolio management. The following provides a description of the DoD GIG architecture, brief descriptions of DoD's relevant strategies, and a discussion of how the Department uses the architecture to drive the three primary Departmental processes – 1) capability and derived requirements, 2) budget, and 3) acquisition – to deliver an environment that supports our 21st Century mission.

The Global Information Grid Architecture

The GIG is the organizing construct for achieving Net-Centric operations and warfare in the Department of Defense. The GIG[2] consists of information capabilities – information[3], information technology (IT), and associated people and processes that support DoD personnel and organizations in accomplishing their tasks and missions – that enable the access to, exchange, and use of information and services throughout the Department and with non-DoD mission partners[4]. The principal function of the GIG is to support and enable DoD missions, functions, and operations. Therefore, the way that DoD warfighters, business and intelligence personnel operate must drive the way the GIG is designed, developed, acquired, implemented, and operated.

The current GIG is characterized by organizational and functional stovepipe systems with varying degrees of interoperability and constrained access to needed information. It does not sufficiently exploit the potential of information age technologies, and does not fully support the operational imperative for the right information at the right time. In addition, the current GIG is static rather than dynamic; it cannot quickly adapt to satisfy unanticipated needs and users. Most importantly, the current GIG is not suited to

[2] See DoD Directive 8100.1, GIG Overarching Policy, September 19, 2002, for full GIG definition.

[3] In this document, the term 'information' includes the term 'data', as commonly used in the foundation documents used to develop this document.

[4] Mission partners are non-DoD individuals and organizations that exchange information with DoD users. Examples include allies, coalition partners, civilian government agencies, and non-governmental agencies and organizations including international organizations.

support NCO – it does not support the ability of warfighters and business and intelligence operators to leverage the power of information.

The current GIG (people, processes, and technology) must be transformed to enable and support DoD missions and operations in a net-centric environment (NCE). The NCE with its attributes and characteristics is the operating environment in which all DoD missions and operations will take place. Major improvements in situational awareness, interoperability, combat operations cycle time, agility, collaboration and the ability to self-coordinate in a NCE enhance military effectiveness and, most importantly, save lives.

The GIG as a Vision, Entity, and Architecture

The GIG as a vision is described in Section 4, Target Capability View, which describes the GIG Architectural Vision.

As an entity, the GIG comprises many systems that interoperate to provide the right information to the right places when needed. Thus the GIG could be considered analogous to a secured World Wide Web (WWW): many systems distributed worldwide that interoperate to allow vast amounts of information to be readily pulled by anyone or anything; anywhere, anytime; if appropriately authorized. In the same manner that the WWW has transformed industries and societies on a global scale, the GIG will support the transformation of our warfighting and business practices.

The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:

- Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.
- Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.
- Processes data or information for use by other equipment, software, or services. Non-GIG IT is stand-alone, self-contained, or embedded IT that is not and will not be connected to the enterprise network.

The GIG is also a well-established and documented architecture that serves as the enterprise level 'blueprint' for information environment. As such, the architecture represents the structure of GIG components, their relationships, and the principles and guidelines governing their design, operation and evolution over time. The responsibility for GIG development and maintenance is shared among several OSD and DoD Components with the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DoD Chief Information Officer (CIO) providing direction, oversight, affirmation, and remediation. The DoD CIO will appoint a GIG Chief Architect to develop and manage the infrastructure and processes to govern the development, maintenance, and use of the GIG Architecture and to establish and implement GIG Architecture configuration control processes.[5] Draft DOD Directive 8010.aa, *Global Information Grid (GIG) Overarching Policy* provides the oversight and governance structure.

GIG Architecture v1.0, the "as-is" architecture, was published in 2003 followed by GIG "to-be" Architecture v2.0, published in 2005. GIG Architecture v2.0 identified the information services needed by the Secretary for decision making in the 21st Century based on various scenarios that seemed likely at the time and was the first attempt to describe a macro view of a Service Oriented Architecture (SOA). From this work flowed the Net-Centric Operations and Warfare Reference Model (NCOW RM), the Net-Centric Enterprise Services (NCES) Program, and the experimental work at Defense Information Systems Agency (DISA) on the SOA foundation, all of which reflect updates to the federated baseline architecture and shows progress toward the target Net-Centric environment, represented in a federated objective architecture.

Each of the Service's major Net-Centric transformation initiatives; the Army's LandWarNet, Air Force's C2 ConstellationNet and the Department of the Navy's ForceNet initiative are currently developing architectures that are required by the Department to be in conformance with the GIG Architecture. In addition, critical core enabling programs such as the Air Force's Transformational Communications System, and DISA's NCES programs must also conform to the GIG Architecture. The Joint Task Force architecture developed by the Joint Forces Command provides a construct against which Service, Agency, and Combatant Commander programs and initiatives are measured for operational sufficiency.

As a result of the work done on the GIG Architecture, the Department is making progress on several programs/efforts key to the NCE, including a program to provide an integrated communications layer within the GIG that increases connectivity and eliminates bandwidth as a constraint programs to provide the basic infrastructure and protection services required to effectively operate the GIG. The Department is also making progress for determining when other significant Information Technology (IT) initiatives, especially in storage, applications, or computing, will advance or take advantage of net centric capabilities.

[5] Draft DODI 8240.aa, GIG Configuration Management and DODI 8210.aa Global Information Grid (GIG) Architecture Development, Maintenance, and Use

The Department is working to extend these transformations to our allies, initially using legacy systems, but including them in our transformation as quickly as we can via Multinational Information Sharing initiatives.

Segment architectures that represent DoD mission areas are in various processes of development. As previously discussed, the BEA is the segment architecture for the BMA. The other mission areas of the Department are building on the success and lessons learned by the BMA and are developing similar segment architectures that conform to and become a part of the GIG. For example, the EIEMA has developed an architecture development structure similar to that used for the BEA and has drafted the Computing Infrastructure segment. The WMA has formed an initial governance structure and is in the process of creating its architecture development structure. DIMA is in process of developing an EA this year. The common approaches employed by each segment will enhance the Department's ability to integrate architectures and avoid unnecessary duplication of effort. DoD segments are incorporating those elements across all DoD Component architectural development efforts to ensure that the resulting products are supportive of and extensions to the GIG Architecture. As this DoD EA Transition Strategy is being developed, DoD is phasing out some of the concepts such as Mission Area IT Portfolio Management in order to align with a DoD-wide capability-based concept initiated by the 2005 Quadrennial Defense Review (QDR). This new concept is described in the Portfolio Management portion of this DoD EA Transition Strategy in the Current Status section. Because this new concept is still in the evolution phase, the remainder of the document will describe the current status of Mission Areas for IT Portfolio Management.

Figure 1 shows the relationship between the OMB layers or tiers and the DoD tiered approach, as shown in Draft DODI 8210.aa, *Global Information Grid (GIG) Architecture Development, Maintenance, and Use* and the *DoD GIG Architecture Strategy*.

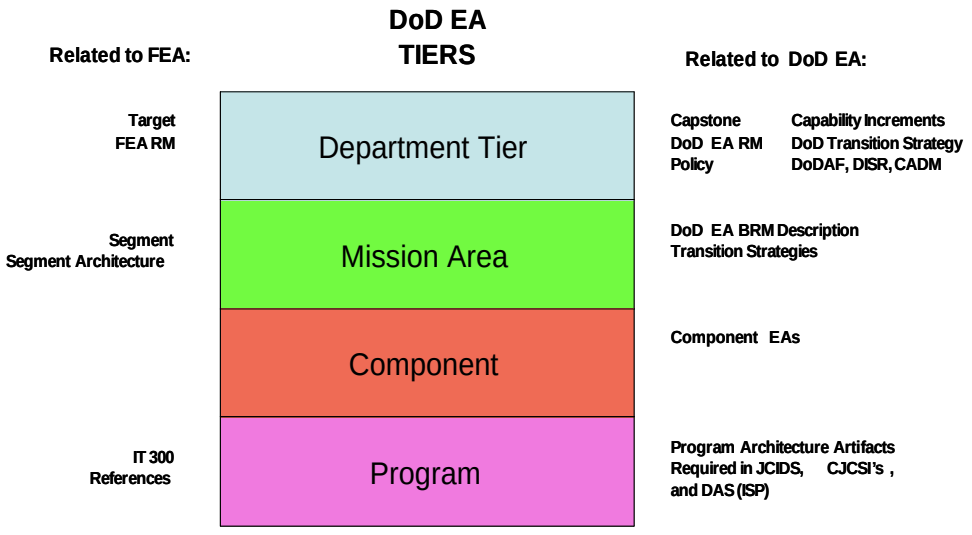


Figure 1 – DoD EA Relationship to OMB FEA

In addition, a snapshot of the federated GIG Architecture may be captured at any point in time as reflected in the DoD EA taxonomies that align information extracted from the federated GIG Architecture and maps that information to the Federal Enterprise Architecture Reference Models (FEA RMs). The relationship of DoD EA with the FEA RMs is described later in this section.

To summarize, considerable progress has been made since GIG Architecture v1.0 and the Department is now institutionalizing this progress through new policies and redefined processes.

From a policy standpoint the DoD Architecture Framework (DoDAF), has an interim update (v1.5, April 2007), which is a transitional version applying essential net-centric concepts[6] and addressing the immediate net-centric architecture development needs of the Department while maintaining backwards compatibility with DoDAF v.1.0. As described in the DoDAF Progress Update of January 2008, the DoDAF will evolve further towards architecting a Net-Centric environment for a SOA in v2.0, scheduled for completion in November 2008.

From a process standpoint, the DoD EA Summit, led by ASD(NII)/Architecture & Interoperability (A&I) Directorate, provides the primary cross component governance and integration of architectures across the Department and among the Intelligence Community.

Finally, The Department has implemented enterprise-wide systems engineering via the Draft DoDI 8230.aa, *Global Information Grid Enterprise Engineering*, to ensure that programs technically comply with the GIG Architecture and its supporting elements noted above. This system engineering activity is being complemented with a GIG end-to-end evaluation (test bed) facility at the Joint Warfighting Center. This facility will be used to ensure that systems being developed by DoD components meet GIG Architectural requirements and its associated Technical Standards as contained in the DoD IT Standards Registry (DISR). The Net Centric Implementation Document (NCID) suite addresses transport, services, data, applications, computing infrastructure, IA, and NETOPS.

DoD Strategies

DoD Strategic Plan

DoD's information vision empowers users through easy access to information anytime and anyplace, with attendant security. To do this, the Department provides a comprehensive information capability that is global, robust, survivable, interoperable, secure, reliable, and user driven. This is the enabling foundation for the Department's Defense Strategy.

[6] NetCentric Concepts are: 1) Populate the Net-Centric Environment, 2) Utilize the Net-Centric Environment, 3) Accommodate the Unanticipated User, 4) Promote the Use of Communities of Interest (COI), 5) Support Shared Infrastructure.

1. The ultimate achievement of this vision depends on the development, deployment, and integration of an effective GIG. Achieving this vision requires changes in doctrine, organization, training, materiel, leadership/education, personnel and facilities (DOTMLPF). The current *DoD CIO Strategic Plan 2006*, sets nine focus areas for the Department:

The 2006 DoD CIO Strategic Plan identifies actions that are critical to transforming DoD operations from platform/organization-centric to Net-Centric. The strategy encompasses doctrine, organization, training, materials, leadership and education, personnel, and facilities (DOTMLPF) implications for making information available on a reliable and trusted network populated with new and dynamic information.

The *Draft Information Management and Information Technology (IM/IT) Strategic Plan*, currently in the review process, will supersede the 2006 DOD (CIO) Strategic Plan V1.0 as described above as well as the June 2004 *DoD CIO Strategic Plan for Information Resources Management.*

The *IM/IT Strategic Plan* is being developed collaboratively with the CIOs of the Military Departments (MILDEPS), Defense Information Agency (DISA), National Security Agency (NSA), United States Strategic Command, and Joint Chiefs of Staff to provide a common understanding of shared vision, mission, and governing principles for IM and IT. The plan identifies six specific goals and objectives to guide the net-centric transformation of the Defense information enterprise during the period 2008-2009. It also defines key performance indicators for assessing progress toward meeting the goals and objectives that will move the Department's net-centric transformation from concept to reality.

Goal 5: Return on Investment in the Draft IM/IT Strategic Plan is to "institutionalize IT PfM and EA to maximize the contribution of IT investments to national security and defense outcomes". The related objectives in the IM and IT Plan are:

- All IT investments are aligned with DoD's overall outcome goals and priorities, and warfighter requirements
- Processes systematically maximize the value of IT investments, and assess and manage the risks of IT acquisitions.
- The IT investment environment is performance- and results-based.
- A federated DoD EA facilitates management and planning of IT investments to achieve improved mission performance.

DoD EA Federation Strategy

The development of a DoD Federated EA will be conducted in accordance with both DoD and Federal policy on the development and use of enterprise architectures. The approach to federation in the *GIG Architecture Federation Strategy* of 01 August 2007 closely follows DoD policy and directives on Net-Centric data management. Net-Centric references, including the Net-Centric Strategies; DoD Directive 8320.2, Data Sharing in a Net-Centric Department of Defense; OMB EA Assessment Framework 2.2; and

Federal Enterprise Architecture Data Reference Model (FEA DRM) 2.0 will be consulted to ensure compliance with policy.[7]

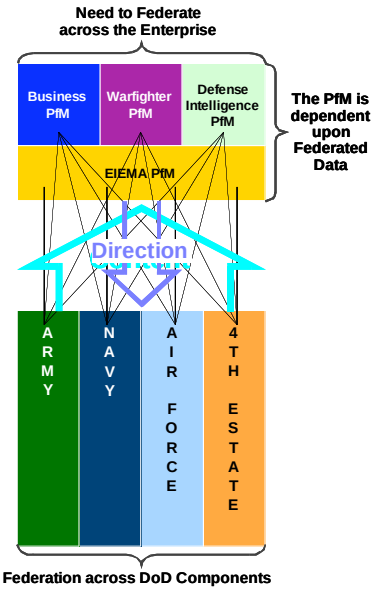


Figure 2 – Federation across DoD Components

The DoD Federated EA directly relates to the development of transition plans as both utilize the federated approach to information sharing. Net-Centric principles for the DoD Federated EA that must be adhered to, including visible, accessible, understandable, and trusted data assets, enabled to support interoperability, require the same types of policies and processes needed for an effective DoD EA Transition Strategy.

The GIG Federation Strategy recommends that agreements be reached within the DoD EA Community of Interest (COI) or Community of Practice (COP) on the structure and semantics of data elements used for data asset discovery, linking, exchange, and integration. Metadata elements needed to support the EA user services described herein are defined and proposed for DoD EA COI/COP acceptance as the standard for Net-Centric federated EA services.

Figure 2 is a high-level view of the DoD information enterprise. **Figure 3** decomposes the high-level view and depicts the interdependencies at all levels of the enterprise. This federated approach enables effective and efficient executive-level decision-making.

[7] DoD Federation Strategy, 16 October 2006

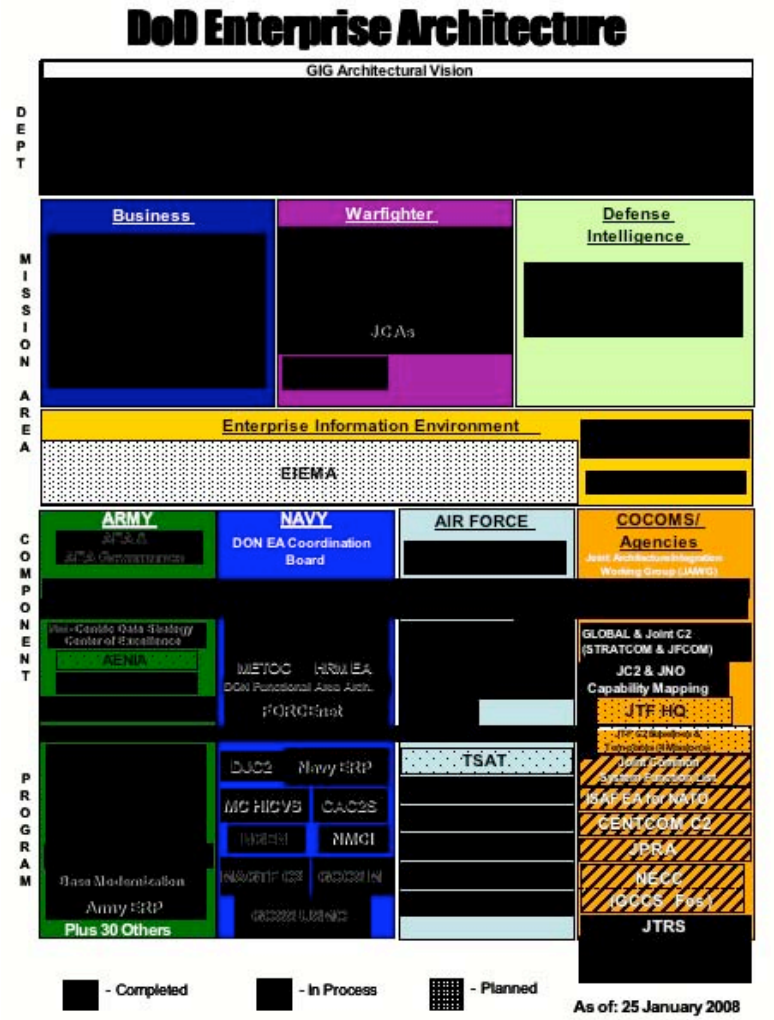


Figure 3. DoD Information Enterprise

DoD Portfolio Management

The DoD IT portfolio management policy[8] and the GIG Architecture support the Department's budget process, directly guiding the resource allocation for IT investments. The GIG Architecture will be used to define critical interrelationships among portfolios and to determine which IT investments within and across portfolios should be supported. Other criteria include:

[8] DODD 8115.01, IT Portfolio Management (10 Oct 2005) and DODI 8115.02 (30 Oct 06) Information Technology Portfolio Management Implementation.

- relevance of an IT proposal to the Department's core mission, priorities, and strategic planning goals
- support to functional area goals and objectives
- return on investment for business initiatives
- soundness of plans for managing, mitigating or diversifying risks
- optimization of resources through eliminating stove-piped development and redundant services and systems

The DoD IT portfolio is comprised of investments in the four areas of DoD: WMA, BMA, IMA, and EIEMA. For the WMA, for example, a set of Joint Capabilities Areas (JCAs) have been defined as of January 2008 to provide a mechanism to manage portfolios across domains within the WMA. They are providing the foundation for the WMA Architecture which, as part of the federated GIG Architecture, will provide authoritative information to the DoD EA RMs. The four Mission Area EAs are discussed further in the Segment Architecture section of this document.

There are nine JCAs in Tier 1 with related Tier 2 and 3 JCAs. The Joint C2 portfolio contains warfighter and user applications to support C2, logistics, and battlespace awareness. This portfolio includes programs such as the Net-Enabled Command Capability (NECC) and the Global Command and Control System (GCCS).

In addition to supporting the Department's budget process, analysis of applications within the C2 Portfolio (C2 Data Pilot) has resulted in a proposal to strengthen the NR-KPP by including data exposure criteria and service exposure criteria.[9]

As the DoD EA Transition Strategy is being developed, DoD has begun phasing out some concepts such as Mission Area IT Portfolio management in order to align with a DoD-wide capability-based concept initiated by the 2005 Quadrennial Defense Review (QDR). Concurrently, DoD has introduced the concept of the Defense Information Enterprise as an organizing construct to differentiate the network infrastructure roles of ASD(NII) from the broader, more encompassing information management role of the DoD CIO. A description of the evolution from Mission Area IT Portfolio Management to capability-based Portfolio Management is included in the paragraph below, *GIG Governance Structure Current and Planned.*

Joint Capabilities Areas

JCAs were first proposed in the 2003 Joint Defense Capabilities Study, also referred to as the Aldridge Study. It called for dividing the Department's capabilities into manageable capability categories as an essential early step to implementing a capabilities-based approach. The study recommended dividing capabilities along functional or operational lines and favored functional categories. Functional categories minimize redundancies in capability decomposition, provide clearer boundaries to assign weapon systems, and improve management ability to develop and implement capabilities planning.

[9] Proposal is before the JROC (Dec 2007)

In 2005, the Joint Force Capabilities Assessment sub-study (Part of the Operational Availability-05 Analytic Agenda) developed the initial 21 Tier 1 JCAs, and developed draft Tier 2 JCA candidates. A subsequent Secretary of Defense memo approved them for "use as appropriate", and referred to them as "the beginnings of a common language to discuss and describe capabilities across many related Department activities and processes." Two separate JCA refinement efforts were conducted, and resulted in the 24 Aug 06 Joint Requirements Oversight Council (JROC) approval of the first JCA taxonomy and lexicon which comprised 22 Tier 1 JCAs and 240 subordinate JCAs.

The JROC also approved a deliberate way forward to enhance the nascent JCAs' utility across the Department. Recognizing the current JCAs were devised mostly on theory and without benefit of practical JCA application, the JROC agreed a baseline reassessment was necessary. Although the JCAs have been through several refinement cycles, the basic JCA framework has only changed on the margins. This baseline reassessment affords the opportunity to holistically improve the JCAs by applying lessons learned from their use in numerous department processes.

The most recent version of the JCAs was approved by the JROC and by the DAWG in January 2008; the set of JCAs is included in the *Consolidated Taxonomy_4 Jan 2008*.

Joint Network Operations

Joint Network Operations (JNO) is another ongoing effort that focuses on key Programs of Record that have the most impact on providing capability to the war-fighters. The JNO Capability Portfolio Manager (CPM) develops architecture products that support analysis and risk assessment efforts needed by CPM decision makers. The architecture factors in Transport infrastructure, Information Assurance, Network Mgt, and Enterprise Services. The architecture products are developed through specific tools that are able to interface with a relational database and other input mechanisms. The database is used to define data models and relationships that ensure data integrity. Products are exported in formats such as NetViz views (dynamic and static), as well as other common formats such as PowerPoint, Excel and bitmap images.

The architecture products developed along with the analysis and risk assessment processes have been instrumental in providing decisioning products to support the POM and other processes.

GIG Governance Structure Current and Planned

Portfolio management responsibility for the Department is currently in four logical management areas – the WMA, BMA, IMA, and EIEMA. Managing these horizontally and vertically requires a federated approach and the Department has a portfolio management approach across the four mission areas and across DoD Components. This is the initial step toward development of a NII/CIO Governance Structure that will provide an overarching integrated approach and a management process that places the GIG under configuration control. To continue toward a governance framework, a long term process is being established and socialized to accomplish the following:

- Organize and focus NII/CIO direction for IT development by promulgating a governance process through policy and institutionalized processes.
- Communicate to DoD Components what is needed.
- Empower DoD Components and then hold them accountable for implementation.
- Discipline GIG development.

An Enterprise-wide approach is being pursued to ensure that the Department's information and information technology management initiatives are planned and managed in a rational way that respects the culture, laws and authorities, such as the Title 10 authorities of the Military Departments and the Goldwater Nichols Act, which gave authorities to the Joint Chiefs of Staff to prepare the force to fight jointly. Together, these authorities establish a matrix organization with the Secretary setting at its head to mediate disputes, build consensus, and provide direction to both the vertical organizations and the horizontal organizations represented by the Mission Area Managers.

This year DoD has introduced the concept of the Defense Information Enterprise as an organizing construct to differentiate the network infrastructure roles of ASD(NII) from the broader, more encompassing information management role of the DoD CIO. The Defense Information Enterprise comprises the information, information resources, assets, and processes required to achieve an information advantage and share information across the Department and with mission partners.

Concurrently, DoD has begun phasing out some concepts such as Mission Area IT Portfolio management in order to align with a DoD-wide capability-based concept initiated by the 2005 QDR. DoD has piloted Capability Portfolio Management (CPM) and has specified a structure whereby all DoD investments (not just IT) will be managed in a series of portfolios. As part of this structure, the ASD(NII) has begun managing the Net-centric capability portfolio focused on IT infrastructure. The DoD CIO supports all CPM portfolios by continuing to specify policies and architectures, and is now also enhancing policy alignment mechanisms.

As a consequence, ASD(NII)/DoD CIO is realigning some management constructs. The current two IT portfolio management efforts (EIEMA and Joint Network Operations) will merge into a Net-centric CPM structure. That portfolio will encompass IT infrastructure investments across all DoD Components. In parallel, the DoD CIO will lead a broadened net-centric review process spanning all programs delivering IT capability (across all portfolios), and focused on ensuring that each IT investment provides visible, accessible, understandable, and trusted net-centric information.

In this vein, the *Defense Information Enterprise Architecture (DIEA)* now provides a common foundation to support accelerated Department of Defense (DoD) transformation to net-centric operations and establishes priorities to address critical barriers to its realization. DIEA 1.0 highlights the key principles, rules, constraints and

best practices drawn from collective policy to which all applicable DoD programs, regardless of Component or portfolio, must adhere in order to enable agile, collaborative net-centric operations.

Note: For the purpose of this DoD EA Transition Strategy, the DoD Mission Area concept is included as the current configuration for DoD IT Portfolio Management. An overview of the Defense Information Enterprise and the DIEA 1.0 as an embedded document is incorporated into this Transition Strategy in the Segment Architecture portion to provide information on the evolution of this concept. Future versions of the Transition Strategy will reflect the detail of changes to the capability-based concept and the evolution of the Defense Information Enterprise versus the EIEMA concept.

DoD CIO Policies

The current *DoD EA Strategic Plan* is being updated to the *Information Management/Information Technology Strategic Plan*, to be released in early 2008. The IM/IT Plan is discussed in more detail above.

Continuous process improvement (CPI) is a DoD transformation initiative highlighted by the words of the Deputy Secretary of Defense Gordon England's statement, *"The Secretary and I expect that every DoD organization is focused every day on **improving the effectiveness** of our support to the Warfighter".* DoD published the *Continuous Process Improvement Transformation Guidebook*, 12 May 2006, for implementing the continuous improvement activities that accomplish this goal.

In conjunction with the Governance Structure, the NII/CIO is in the process of updating several DoD CIO series 8000 policies in the areas of control, content, coordination, and compliance to both consolidate existing policies in a logical configuration and to make necessary changes to reflect current linkages to DoD CIO goals and objectives. The relevant DoD 8000 Series are being updated in a collaborative process and are currently in the SD-106 review process. These policies, in addition to existing policies, include direction for DoD organizations and entities in regard to enterprise architecture development, maintenance, and measuring processes, such as the IT300 and OMB and GAO EA assessment.

Existing DoD CIO policies address all areas of EA and processes and include the DoD Series 8000 guidance and Mission Area (MA) EAs, such as the Business Enterprise Architecture (BEA) and the Enterprise Information Environment MA Architecture (EIEMAA). Additionally, DoD follows the Office of Management and Budget (OMB) A-11 guidance and has institutionalized the IT300 submission process and the OMB EA Assessment process.

The DoDD 4630.5 and DoDI 4630.8, Information and Supportability of Information Technology and National Security Systems, is also currently being updated from May 2004. There are two levels of updates, one scheduled for Fall 2008 and one for Spring 2009.

The intent of updating the policies is to provide the foundation for organizing, focusing, and articulating what the NII/CIO does (GIG management, governance, oversight) and what the Components do (develop GIG capabilities – content) in accordance with broad policy direction. The policy will then establish processes for the NI/CIO governance role and the Components' accountability requirements.

The DoD EA Transition Strategy uses the elements of the Governance Structure as part of the entire lifecycle of a DoD portfolio. The identification of the GIG Capability Increments and the related milestones are critical to bring the GIG vision into reality. **Figure 4** details the GIG Lifecycle.

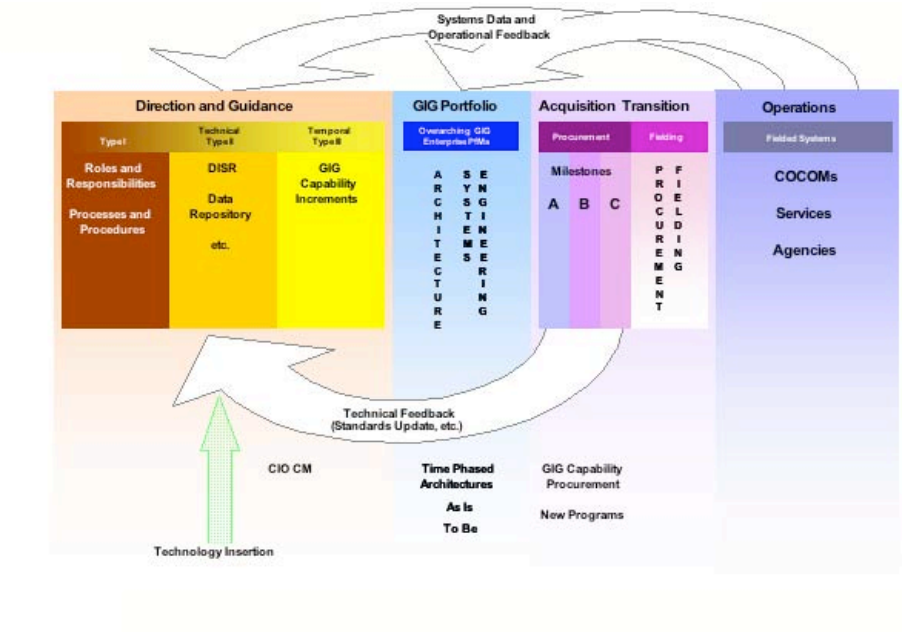


Figure 4 – The GIG Lifecycle

The GIG Architecture Drives Departmental Processes

As previously stated, architecture plays an increasing role in three of the Department's primary business processes: capability setting, budget and acquisition. In fact, the requirements and acquisition processes have recently been reengineered to make better use of architectures for decisional purposes.

The requirements process, Joint Capabilities Integration and Development System (JCIDS), uses the GIG Architecture description of information technology as the authoritative view of interoperability and information assurance for use in defining Joint capabilities. The mandatory Net-Ready Key Performance Parameter (NR-KPP) increases the Department's emphasis on information assurance and data interoperability through the NCOW RM in formulating specific NR-KPPs for new programs. Compliance with the NR-KPP requires the proposed capability be able to enter and be managed in the network and exchange data in a secure manner. NCOW

RM terminology must be included within architectural views provided with the capability.[10] The NR-KPP is a key part of the IT and NSS Interoperability and Certification process. These associated architecture products in JCIDS documents provide the details to conduct detailed traceability analysis which feed decisions on programs.

Joint Functional Concepts (JFCs) and Joint Integrating Concepts (JICs) provide targeted guidance for capability development. The NCE JFC provides a framework for full human and technical connectivity and interoperability that allow all DoD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence; protecting information from those who should not have it. The Net-Centric Operating Environment (NCOE) JIC defines coherent application of seamless, integrated Net-Centric capabilities to the forward edge of the battlespace enabling full spectrum dominance.

In the DoD Acquisition Process, the GIG Architecture is recognized as the underpinning for all mission and capabilities architectures developed by the Services and DoD Agencies. The Department also requires the development of GIG-conformant Information Support Plans (ISPs) that detail information interoperability and content needs and dependencies of individual programs. These ISPs are also used to evaluate program interoperability and lifecycle management.

DoD Net-Centric Strategies

The OMB Assessment Framework for the Department of Defense for FY07 noted that the DoD Net-Centric Strategies need to be completed for overall maturity of the DoD EA. The intent of the Net-Centric Strategies is to provide important overall guidance to managers on how to include these areas in their program plans, goals, and objectives that will help to develop transition plans that comply with DoD Net-Centric goals and objectives.

The Senior Enterprise Services Governance Group (SESGG) is a governance mechanism for Joint Data and Enterprise Services, co-chaired by the DoD Chief Information Officer (CIO) and the Director National Intelligence (DNI) CIO. The SESGG defines the required measurement and control mechanisms to ensure DoD-wide and IC-wide implementation of the Data Strategy and Enterprise Services. The SESGG also identifies and develops necessary policy changes, including measurement and control responsibilities, to ensure consistent implementation of the Data Strategy and enterprise services. Lastly, the SESGG establishes oversight forums to enable the DoD CIO and the DNI CIO to review implementation progress. The SESGG members include representatives from the Army, Navy, Air Force, U.S. Marine Corps, DISA, Defense Intelligence Agency, and BTA.

This section captures the overarching DoD CIO strategy, casts the historical context that proved the impetus for the subsequent strategy documents, and highlights the

[10] CJCSI 6212.01D, Table D-2

intent and the salient points of the various DoD strategy documents' guidance that support a pragmatic approach to IT implementation of the respective strategy.

Historically, IT resources and software-based capabilities have been acquired and managed as stand-alone systems; namely, system-to-system connections are defined, engineered, and implemented one pair at a time – an approach that focuses on system or platform capabilities rather than on mission capabilities. With respect to data, the traditional DoD approach was data administration; namely, to standardize and control data definitions and structures across the department. With respect to sharing, the supply and demand for information continually triggers the inter-related processes of information collection, processing, analysis, and integration to make informed to increase situational awareness and to make informed timely decisions. With respect to NetOps, a set of stove-piped disparate and manual processes breed limited information sharing and integration, non-standard configuration management and metrics, and relatively static configurations. As a result, DoD promotes and encourages 'new' paradigms that expose capabilities, establish data visibility and accessibility, and fosters information sharing as well as synchronization in its information sharing initiatives and investments throughout the Department.

With respect to network protocol, in the GIG, IP is the common network protocol that allows all types of data to move seamlessly on the GIG's diverse transport layer which includes landline, radio, and space-based elements. The current version of Internet Protocol (IP), IPv4 has limitations that inhibit the end-to-end paradigm of the internet and achievement of DoD's vision of net-centric operations. The numerous "fixes" and extensions implemented to overcome IPv4 limitations often have increased network complexity and slowed network performance. Finally, a fully connected environment - specifically, an implementation of highly integrated wireless architectures and spectrum dependent technologies (weapons, sensors, geo-locators, etc) – that instruments and networks the battle-space must fit within the context of these new paradigms which significantly increase the war-fighters dependence on spectrum.

DoD Net-Centric Data Strategy

The *DoD Net-Centric Data Strategy 09 May 2003* describes a vision for a net-centric environment and the data goals for achieving that vision. It defines approaches and actions that DoD personnel will have to take as users—whether in a role as consumers and producers of data or as system and application developers. The strategy reflects a "...many-to-many exchange of data, enabling many users to leverage the same data – extending beyond...focus on standardized, predefined, point to point interfaces... and without having to anticipate...use in the development cycle..." More pointedly, the strategy defines a modified paradigm for data management.

Data implies all data assets (e.g., file systems, databases, documents, images, audio files, web sites, etc). The goal is to post before processing; i.e., make visible and accessible raw data. In the Net-Centric Data environment authorized users and applications have immediate access (via "pull" as needed). Users and applications

providing data post and tag the data assets with metadata to enable discovery on the Enterprise' shared space.

Key components of the data vision are Communities of Interest (COI), Metadata, and GIG Enterprise Services (GES). COIs are collaborative groups of users with shared goals, interests, missions, or business processes and therefore must have shared vocabulary for the information they exchange. Metadata is data about data and can enhance the value and usability of data assets as well as aid in the advertisement of the data asset within the enterprise. Types of metadata are discovery (summarizes key attributes and concepts), vocabularies, taxonomic structures, interface specifications, and mapping tables. Various mechanisms are utilized to store the various types of metadata including registries, catalogs, and shared spaces. Definition, how to use, and when to use each mechanism is described in the data strategy. GES provides basic computing capabilities to the enterprise. The GES capability is the DoD Metadata Registry based on ISO 11179 Specification and currently incorporates the extant DDDS and DoD XML Registry with planned integration of ontology, transformation services, and messaging formats.

Approaches to achieve the Data Strategy Goals are detailed in the strategy. All approaches should be coordinated with IA and GIG infrastructure; COIs should be utilized to prioritize system and data transition and eliminate redundancy.

To enable the DoD Data Strategy and to provide capabilities for Communities of Interest (COIs) to accomplish its goals, the DISA PEO-GES provides tools, techniques, and performance standards at the DoD Metadata Registry (MDR) website, https://metadata.dod.mil/mdr/documents.htm. The website hosts the DoD MDR as well as briefings, documents, Metadata Working Group archives, and supporting NCES initiatives information.

The DoD MDR Version 6.1 is an implementation of the Data Strategy per the 24 Oct 2003 DoD CIO Memorandum *DOD Net-Centric Data Strategy: Visibility – Tagging and Advertising Data Assets with Discovery Metadata* and the DoDD 8320 .02 of May 2004, *Data Sharing in a Net-Centric Department of Defense,* which directs the use of resources to implement data sharing among information capabilities, services, processes, and personnel interconnected within the GIG.

The DISA PEO-GES, in support of Component planning and implementation to achieve data visibility provides the following on the website:

- A description of the functions and the concepts of operations for DoD Enterprise Discovery including specific implementation details and guidance on discovery of Services, Content, Metadata, and Persons. This whitepaper will provide sufficient detail to enable DoD Components to understand Enterprise Discovery capabilities and factor them into transition planning.
- A set of specifications (including required service levels) that describe Enterprise Discovery functions and their interfaces to enable federation with

Component discovery capabilities. These interfaces should incorporate the DoD Discovery Metadata Specification.

- A reference implementation of the interfaces provided in Action (b) that exemplifies how Community of Interest Discovery capabilities can federate with Enterprise Discovery.

A July 2007 briefing, *DoD Information Sharing Metadata Efforts* by Dr. Glenda Hayes, of the DISA PEO-GES, gives explicit examples of realizing the DoD Data Strategy goals including an animated detailed Federated Search Use Case for information sharing within and between programs of record (PORs) and COIs. Finally, illustrations of online tutorials are included; specifically, *Registering Metadata* and *Version 6.1 DoD Metadata Registry (MDR) functionality*.

DoD Net-Centric Services Strategy

The *DoD Net-Centric Services Strategy 04 May 2007* describes the DoD's vision for establishing a Net-Centric Environment (NCE) and expands upon the DoD Net-Centric Data Strategy by connecting services to the Data Strategy goals. The commercial world defines business processes as workflows that consist of specific business functions that are supported by the delivery of software-based services over networks. These software-based services deliver reusable business functionality as standardized building blocks on an enterprise network.

A simplified workflow for a DoD business process, inventory management, is depicted in **Figure 5**. The function, "Check Forward Supply" is implemented using software building blocks or services (e.g., a Get Inventory Count service) and provides a distinct element of functionality that can be used in other processes by Military Services, Agencies, Commands, or mission partners. When a new mission capability is required (e.g., needing a new business process for logistics planning for a mission planning application), the Get Inventory Count building block can be quickly used to respond to this new or changing mission need.

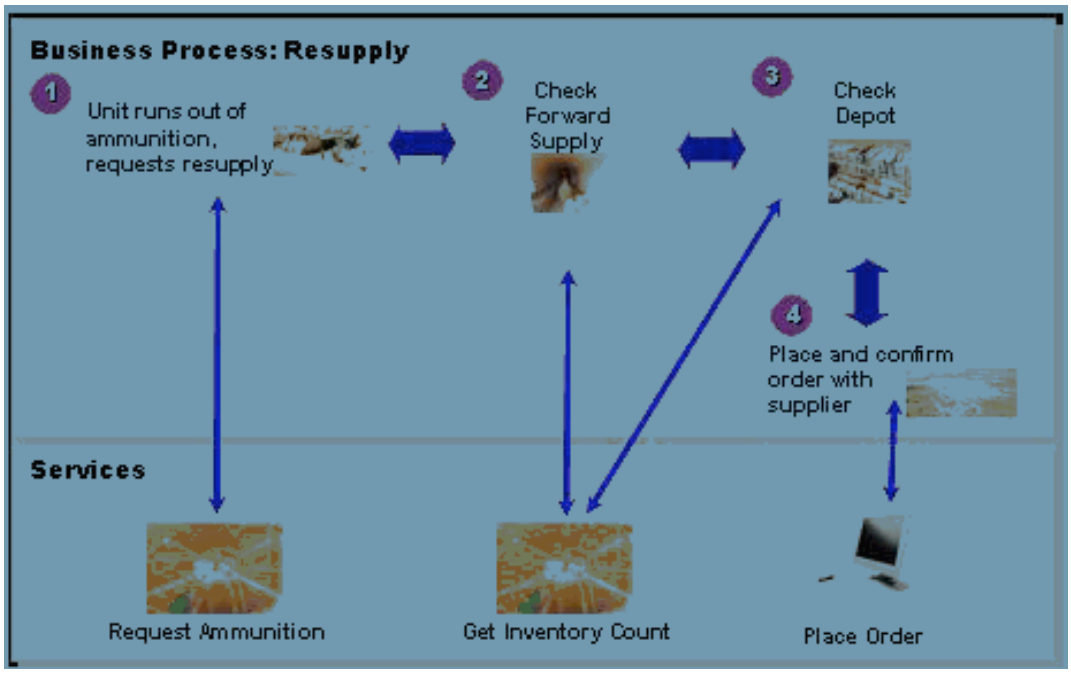


Figure 5. DoD Business Process Workflow

This approach lies at the core of a Service Oriented Architecture (SOA). As the Department transforms towards net-centric operations, the DoD NCE will increasingly leverage shared services and SOAs that are supported by the required use of a single set of standards, rules, and a common, shared secure infrastructure provided by the Enterprise Information Environment Mission Area (EIEMA) and populated with appropriately secure mission and business services provided and used by each Mission Area. Of the four goals, "provide services" is the most user focused. Specifically, as the NCE evolves, users will provide their information and functional capabilities to the enterprise as services. Providers of services must register their services in the enterprise service registry (i.e., publish the metadata describing their services). Core Enterprise Services (CES) are a small set of services to be provided by EIEMA.

DoD Information Sharing Strategy

DoD Information Sharing Strategy 04 May 2007 documents the common vision to synchronize information sharing initiatives and investments throughout the DoD in order to leverage information as a strategic asset in achieving the DoD mission. Information sharing is the means by which information is shared ranging from face-face interactions to real-time voice communications and beyond across trusted networks. The strategy guides the information sharing within the DoD as well as with Federal, State, local, tribal, coalition partners, foreign governments, and private sector. Of the five touchstones of information sharing, Technology and Infrastructure are the most relevant for realizing the technology focus of the DoD transition strategies. A companion DoD Information Sharing Strategic Implementation plan describes the specific roles, actions, responsibilities and milestones.

Goals which rely on technology are 'strength agility' and 'ensure trust' by implementing adaptive technologies and accommodating different levels of trust, respectively. Approaches to achieving the goals that rely on technology are 'forge information mobility' and 'promote a federated information sharing community/environment' by requiring trusted (authenticated, confidential, non-repudiated, and integrity) information to be visible, accessible, and understandable and includes trust mechanisms, standards, procedures, and audit regimes, respectively. Finally, implementation considerations information delivery, collaboration, and information and knowledge management advances as well as current and innovative standards based (i.e., comply with the DoD and Federal Enterprise Architectures) technology will enable information sharing in the Technology and Infrastructure domains.

DoD Net-Centric Information Assurance (IA) Strategy

The bulk of the *DoD Net-Centric Information Assurance (IA) Strategy circa 2004* addresses the strategic approach to network IA and has six goals and several associated objectives. In general, secure engineering should be consistent with the IA architecture, policies, standards, and implementation guides. In remaining consistent with the purpose of this section, the 'Protect Information' goal is highlighted here. 'Protect Information' stresses that one cannot rely on simple transport/link encryption given that a net-centric concept means information flows in and out of the network at numerous access points. Hence, a secure labeling and marking of data ("tagging") is necessary to ensure agility for dynamic access control decisions. This includes strong built-in authentication and authorization considerations so that devices that can be reconfigured for security or functionality purposes without human intervention.

DoD Net-Centric NetOps Strategy

The *DoD NetOps Strategy*, 14 December 2007, defines NetOps, its provisions, and intent. NetOps is the "…Department-wide operational, organizational, and technical construct for operating and defending the GIG and provides commanders with GIG situational awareness and C2 capabilities. The intent is to establish a net-centric capability for dynamically operating and defending the GIG as a unified, agile enterprise to enable rapid mission-oriented decisions at appropriate levels across domains. NetOps integrates Enterprise Management, Net Defense, and Content management and assures the availability, protection, and integrity of DoD networks, systems, services, and information. Effectively NetOps results in routine, rapid, and accurate reallocation or reconfiguration of GIG resources in a protected information assured environment. Finally, NetOps records strategic goals and associated objectives and next steps. With respect to next steps, identified requirement is the development and execution of NetOps Implementation plans at all levels across DoD that address three key areas: governance, implementation, and metrics for monitoring, affirmation, and remediation.

DoD Net-Centric Spectrum Management Strategy

This *DoD Net-Centric Spectrum Management (SM) Strategy - 3 August 2006* introduces the vision for this new term which describes an objective capability for the management

and use of electromagnetic spectrum within a net-centric environment. The strategy records the vision, goals and methods for achieving, responsibilities and challenges to Net-Centric Spectrum management. A subsequent directive will detail specific actions and responsibilities to achieve the vision.

In essence, the Net-Centric SM vision is spectrum access on demand enabled through the use of planning, standards, SM protocols, and software agents that will capture the type and amount of spectrum in use and support the most effective use of available spectrum. Goals reflect on-the move access, mitigation of harmful interference, decentralized SM, and autonomous performance throughout the network. Methods for achieving include but not limited to common SM standards and protocols and 'context aware' use (i.e., determine amount of spectrum needed for specific use then select the appropriate spectrum parameters).

DoD Computing Infrastructure Strategy

The *DoD Computing Infrastructure Strategy* (Draft Final, March 2007) is currently being reviewed.

DoD Internet Protocol Version 6 (IPv6) Transition Plan

The Internet Protocol v6 (IPv6) Enabling Program has a transition plan in place, the *DoD IPv6 Transition Plan v.2.* The Defense IPv6 Transition office (DITO) coordinated with DoD Components to develop a DoD-wide, consolidated IPv6 implementation schedule for major DoD networks and programs. The integrated implementation schedule of 4 October 2007 includes specific system IPv6 transition milestones as well as the schedule for accomplishing critical supporting tasks. The DoD Components will update and maintain internal schedules (as part of the DoD Component IPv6 Transition Plan) on a continual basis.

The ASD(NII)/DoD CIO June 9, 2003 memo established a goal to transition DoD network systems to IPv6 by FY 2008. In the August 2, 2005 memo "Transition Planning for Internet Protocol Version 6 (IPv6)," the Office of Management and Budget (OMB) set June 2008 as the date by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure. The implementation schedule defines activities that can be accomplished by the FY 2008 time frame based on three milestone objectives and identifies programs and networks transitioning beyond the FY 2008 goal.

The planning emphasis for FY 2008 has been on transitioning the core DoD network Infrastructure; a timeline for implementation with DoD Teleport is graphically described in the IPv6 Transition Plan.

The *DoD IPv6 Transition Plan June 2006* "…describes the overall strategy for IPv6 transition, identifies roles and responsibilities, outlines transition governance, milestone objectives, and foundation for more in-depth efforts…" Internet Protocol Version 6 (IPv6) is the next-generation network layer protocol for the internet and the Department

of Defense (DoD) Global Information Grid (GIG). Sensors, platforms, and weapons are being built as 'net-ready' nodes incorporating IP-based protocols. Key elements of the plan highlighted here are governance and technical transition. Salient pertinent details of the plan include:

- The most important IPv6 features and associated attributes that facilitate DoD net-centric operations; namely, improved end-end security, Quality of Service (QoS) flexibility, improved mobility, simplified network management, and 'unlimited' address availability;
- DoD components' responsibilities of developing an IPv6 transition plan that includes network transition strategies, transition activities, and timelines and identifying, re-sourcing, engineering, and fielding pilot IPv6 implementations;
- Joint Staff IPv6 key operational and technical items that must be successfully demonstrated for IPv6 transition; all of which are further decomposed into testable and verifiable measures of performance in DoD IPv6 Generic Test Plan Version 3;
- Key IPv6 documentation to be utilized to facilitate DoD IPv6;
- List and expanded treatment of nine IPv6 Transition Elements

Finally, to manage the security challenges and associated risks, the DoD has established a set of milestone objectives; namely, provide DoD Components the authority to operate using IPv6 within approved isolated network domains (enclaves), across cooperative multi-domain environments (transport), and the capability of accepting, routing, and processing IPv6 protocol traffic while providing parity to IPv4. With respect to milestone objective 2, guidance for the transition stage (i.e., when IPv4 and IPv6 are utilized simultaneously) includes architectural, functional, and security requirements as well as recommendations and configuration guidance to implement the aforementioned requirements.[9]

A July 2007 article in CrossTalk magazine, *Spiraling Information Demands – The Way Ahead with IPv6*, was written by the DoD IPv6 Transition Office and outlines IPv6 status and challenges.

Net-Centric Enterprise Solutions for Interoperability (NESI)

Net-Centric Enterprise Solutions for Interoperability (NESI) 12 October 2007 provides, for all phases of the acquisition of net-centric solutions, actionable guidance that meets DoD Network-Centric Warfare goals. NESI provides specific technical recommendations that a DoD organization can use as references. Stated another way, NESI serves as a reference set of compliant instantiations of various directives, policies and mandates such as the Net-Centric Operations and Warfare Reference Model (NCOW RM) [R1176] and the ASD(NII) Net-Centric Checklist. As currently structured, the NESI implementation covers architecture, design and implementation, compliance checklists, and a collaboration environment that includes a repository. More specifically, NESI is a body of architectural and engineering knowledge that guides the design, implementation, maintenance, evolution, and use of the Information Technology (IT)

portion of net-centric solutions for military application. The guidance in NESI is in line with commercial best practices in the area of enterprise computing.

Initial authority for NESI is per the Memorandum of Agreement between Commander, Space and Naval Warfare Systems Command (SPAWAR); Navy Program Executive Officer, C4I & Space (now PEO C4I); and the United States Air Force Electronic Systems Center (ESC), dated 22 December 2003, Subject: Cooperation Agreement for Net-Centric Solutions for Interoperability (NESI). The Defense Information Systems Agency (DISA) formally joined the NESI effort in 2006.

Alignment with the Federal Enterprise Architecture

The Department of Defense aligns with and leverages the Federal Enterprise Architecture RMs (FEA RMs) in several ways. First, the Department maps the FEA RM taxonomies to the four DoD Mission Areas (Business, Warfighter, Intelligence, and Enterprise Information Environment) using DoD architecture and other related artifacts as resources. For example, the activities of the BEA in the BMA are mapped to the FEA BRM Lines of Business (LOB). These DoD taxonomies serve as the business, performance, technical, data, and service component common taxonomies for the DoD Architecture Repository System (DARS), as indicated in the DoD EA Federation Strategy. The use of these taxonomies provides the common terms of reference to achieve internal and external regulatory compliance, interoperability, and net-centricity and ultimately acts as a foundation for improved decision making within and across mission areas. The DoD taxonomies are updated as new DoD resources, such as new versions of an architecture, are released. The draft DODI 8210.aa, *Global Information Grid (GIG) Architecture Development, Maintenance, and Use*, currently in the DoD Directives Program Coordination (SD Form 106) process, mandates the use of common taxonomies.

Second, DoD has developed the DoD EA Consolidated Reference Model (DoD EA CRM) that aligns with FEA categories but uses actual data from DoD investments. The actual data (LOB, mission area, service component, performance information, technical standards and specifications) is derived from the Exhibit 300 input, rather than the generic FEA or DoD taxonomies. The DoD EA CRM therefore serves as a snapshot of the federated GIG architecture by mission area for a sample set of DoD investments. It tracks the line of sight from strategic goals through actual results and can identify gaps and redundancies as well as research, development, and cost sharing opportunities.

Third, DoD leverages the requirements for data from external sources, such as the OMB Circular A-11 guidance for Exhibit 300 and 53 submissions and the OMB EA Assessment Framework, to review and analyze DoD enterprise management information to make recommendations that contribute to more effective and efficient decisionmaking Department-wide.

Lastly, the Segment Architecture aligns with the FEA RM structure and is a way to abstract the business, performance, service component, technical, and data information about a segment or, in the case of DoD, a Mission Area. The Segment Architecture

guidance from OMB, *The FEA Practice Guidance*, and DoD's, *A Practical Guide for Bringing Enterprise Architecture Value to the Mission,* also provides guidance for developing transition strategies and sequencing plans.

Information Sharing Environment and Homeland Security Presidential Directive - 12

The Information Sharing Environment (ISE) and Homeland Security Presidential Directive 12 (HSPD-12) are examples of initiatives in which DoD participates with other federal agencies. The ISE is in the EIE MA; the Line of Business (LOB) is Information Technology and Management and the LOB Sub-Function is Information Sharing. HSPD-12 is in the EIE MA; the Line of Business (LOB) is Information Technology and Management and the LOB Sub-Function is Information Systems Security.

The ISE consists of multiple sharing environments designed to serve five communities of interest (COIs): intelligence, law enforcement, defense, homeland security, and foreign affairs. The ISE represents a trusted partnership between all levels of government, the private sector, and foreign partners, to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the US. The ISE will provide a distributed, secure, and trusted environment for transforming terrorism information sharing into actionable information for community-wide sharing.

The ISE managing partners and cabinet-level Departments and Agencies collaborate and make agreements that influence investments in the set of IT Exhibit 300s (known hereafter as the IT portfolio). The ISE community is currently discussing how to affect the investments in FY09 budget and have begun the necessary planning to accomplish the desired results using the ISE EA Profile and ISE Functional Standard (FS) Suspicious Activity Reporting (SAR).

HSPD-12 directs mandating adoption of a common identification standard (HSPD-12) for all Federal employees and contractors. HSPD-12 is currently being executed. DoD is working with other agencies on follow-up actions, including participation on interagency boards for technical issues, and on the Federal Identity Credentialing Committee for policy issues.

Segment Architecture

Business Mission Area

The BMA has a mature Business Enterprise Architecture (BEA) and an Enterprise Transition Plan, which together comprise the BMA segment architecture. The Business Transformation Agency (BTA) further delineates the architectures, transition strategy, governance, cost savings, IPv6, EA value, and other information to provide artifacts as evidence of Completion, Use, and Results for the OMB EA Assessment. The BMA Segment and all relevant artifacts are included in the BMA EA Self-Assessment as a part of the overall DoD EA Self-Assessment. The high-level descriptions of scope,

vision, change drivers, performance goals, and funding strategy are included in Appendix H.

Business Transformation Transition Plan

The *DoD 2007 Enterprise Transition Plan (ETP)* of September 2007 is an important element of the DoD Transition Strategy as it describes DoD's overall business transformation approach and defined key elements of that approach to include well-defined priorities supported by key systems and initiatives. It aligns transformation priorities to a set of "business value-added measures" to ensure investments are articulated and measured against tangible business value to the Department. Features of the ETP include new and refocused programs that fill operational gaps; rebaselined schedules that reflect revised urgency and adaptation to unplanned delays; and a more complete performance management framework that charts the course toward planned transformation outcomes.[11] Future versions of the ETP will continue to track actual progress toward achieving improvements.

Defense Information Enterprise Architecture

The *Defense Information Enterprise Architecture (DIEA)* unifies the concepts embedded in the many DIEA-driven net-centric strategies into a common vision, providing relevance and context to existing policy. DIEA highlights the key principles, rules, constraints and best practices drawn from collective policy to which applicable DoD IT programs, regardless of Mission Area, Component or portfolio, must adhere in order to enable agile, collaborative net-centric operations. In today's information environment, the DIEA rules clearly apply within the persistently-connected Internet Protocol (IP) boundaries of the Global Information Grid (GIG). Outside of these boundaries, the principles still should be considered, but the rules of the DIEA must yield to the state of technology, and the needs and imperatives of the Department's other Mission Areas. Core principles and rules are organized around five key priorities where increased attention and investment will bring the most dramatic and immediate progress towards realizing net-centric goals.

The DIEA v1.0 is currently scheduled for publication in January 2008. Appendix I in this DoD EA Transition Strategy includes V1.0 of the DIEA. The content of the DIEA and the following high-level descriptions of the scope, vision, change drivers, performance goals, and funding strategy, as defined in the FEA Practice Guidance for transition strategy development, comprise the DIEA Segment Architecture. The high-level descriptions of scope, vision, change drivers, performance goals, and funding strategy are included in Appendix I. See the *GIG Governance Structure Current and Planned* in this Current Status section for more information on the Defense Information Enterprise.

Warfighting Mission Area

The WMA EA Segment Architecture is currently in development in conjunction with the WMA EA. The WMA EA v1.0 is scheduled to be completed in February 2009. To date,

[11] DoD Business Transformation Agency, *2006 Enterprise Transition Plan*, Sep 28, 2006.ibid

the WMA Segment Architecture includes a Project Plan and GANTT Timeline for development as well as Executive Summary and other artifacts. These artifacts provide an interim deliverable that shows progress toward the full WMA Segment Architecture in February 2009. To provide content for the DoD EA Transition Strategy, the high-level descriptions of scope, vision, change drivers, performance goals, and funding strategy are included in Appendix J.

.

Intelligence Mission Area

The Defense Intelligence Mission Area (DIMA) EA is in process of development under the auspices of USDI; Segment Architecture development will progress in conjunction with the EA development. DIMA as an organization currently is working on its fundamental structure, purpose, and direction. The DIMA Vision, Mission, Goals, and Objectives are being rewritten; the DIMA governance structure is being redrafted; there is a pending realignment of DIMA within USDI from DUSD Warfighter Support to DUSD Acquisition, Resources, & Technology that is awaiting a GO/SES-level decision; relationships with ODNI and DIA are evolving; and there is discussion about changing the DIMA's Enterprise Architecture concept to a Business Architecture. DIMA also plans to synchronize efforts with those of the other Mission Areas

The Intelligence Community (IC) EA currently has a Business RM, v1.1 and a Service Component RM v0.8 being developed under the Director of National Intelligence (DNI). The DIMA EA and IC EA development are coordinated efforts.

Cross-Agency Initiative Summary

The Department participates in the President's Management Agenda (PMA) E-Gov Program, which includes a variety of Cross-Agency Initiatives. The following tables describe initiatives in which the Department participates and illustrates the alignment of the initiatives with FEA Lines of Business (LOB) and Sub-Functions by DoD Mission Area. The mapping of the FEA LOB and sub-functions by DoD EA Mission Area are derived from the DoD EA Business Reference Model (BRM).

The tables below (Table 1 and Table 2) provide a view of the Cross-Agency Initiatives that reflect the implementation of common solutions with DoD participation.

Cross-Agency Initiative Tables

Table 1. PMA E-Gov Initiative/Line of Business (LoB)

PMA E-Gov Initiative / Line of Business (LoB)	E-Gov Initiative / LoB Description	DoD Mission Area	FEA BRM LOB	FEA BRM LOB Sub-Function
E-Rulemaking	E-Rulemaking is a Federal-wide electronic system to promote public access to the regulatory process. Allows citizens and organizations to search and comment electronically on rulemaking information.	EIE	Regulatory Development	Public Comment Tracking
Business Gateway	Business Gateway is the official resource to help businesses quickly find compliance information, forms and contacts from multiple gov websites.	EIE	Administrative Management	Workplace Policy Development and Management
Grants.gov	The E-Government Initiative, Grants.gov provides electronic functionality for applicants and grantees, and reduces the paper-based processes that currently challenge the Federal grants environment.	Business	Administrative Management	Workplace Policy Development and Management
Integrated Acquisition Environment (IAE)	IAE is a suite of E-GOV projects that provide information on central contractor registration, performance and subcontract reporting, Federal business opportunities, technical data solutions, online representations and certifications application.	Business	Supply Chain Management	Goods Acquisition
E-Authentication	E-Authentication provides validation services for multiple forms of identity credentials to e-Gov initiatives and other Federal electronic service delivery processes by providing a common, unified authentication service for government-wide use.	EIE	Information and Technology Management	Information Systems Security

Financial Management LoB (FMLoB)	FMLoB goals are to enhance cost savings in for future FM systems, provide standardization of business processes, promote seamless data exchange among Agencies and strengthen internal controls in financial and subsidiary systems.	Business	Financial Management	Reporting and Information
Human Resources LoB (HR LoB)	The vision of the HR LoB is to create a framework for Government-wide, modern, cost effective, standardized, and interoperable HR solutions that provide common core functionality to support the strategic management of human capital.	Business	Human Resource Management	HR Strategy
E-Training	E-Training's vision is to create an environment that supports development of the Federal workforce through simplified and one-stop access to high quality e-Training products and services, and, thus advances the accomplishment of agency missions.	Business	Human Resource Management	Employee Development and Performance Management
Recruitment One-Stop (ROS)	ROS will provide a single application point for agency recruitment needs and support strategic human capital management and affirmative action planning within the legal and regulatory framework and labor management obligations.	Business	Human Resource Management	Staff Acquisition
Enterprise Human Resources Integration (EHRI)	EHRI will eliminate paper records and enable electronic benefits reporting and electronic transfer of HR data throughout the Federal employee's life cycle. It will streamline and improve workforce reporting, data analyses and claims processing.	Business	Human Resource Management	Benefits Management

E-Payroll	The vision of e-Payroll is to accomplish transformation of Federal payroll to provide "Simple, easy to use, cost effective, standardized integrated e-HR/Payroll services to support the mission and employees of the Federal Government".	Business	Human Resource Management)	Compensation Management
Grants Management LoB (GM LoB)	GM LoB is a multi-agency initiative to develop a government-wide solution to support end-to-end grants management activities that promote citizen access, customer service, and agency financial and technical stewardship.	Business	Administrative Management	Workplace Policy Development and Management
Federal Health Architecture (FHA)	FHA is a collaborative environment for Federal agencies to identify common Federal health business requirements and processes, and recommend health data standards for industry to use in building health IT products.	Business	Health	Health Care Delivery Services
Information Systems Security LoB (ISS LoB)	ISS LoB will improve effectiveness and consistency of information systems security across the Federal Government by addressing those areas of information security which are common to all agencies.	EIE	Information and Technology Management	Information Systems Security
Geospatial LoB	Geospatial LoB recommends a set of common Government-wide solutions to serve the interest the Nation and Federal agencies through more effective and efficient development, provisioning and interoperability of geospatial data and services.	EIE	Information and Technology Management	Information Management

Budget Formulation and Execution LoB (BFELoB)	BFELoB will build future budgets employing standards and technologies for electronic information exchange to link budget, execution, performance and financial information throughout all phases of the annual budget formulation and execution cycle.	Business	Financial Management	Funds Control
Information Technology Infrastructure LoB (ITILOB)	ITILOB will identify opportunities for IT infrastructure consolidation and optimization, and develop government-wide common solutions.	EIE	Information and Technology Management	IT Infrastructure Maintenance

Table 2. Other Cross-Agency Initiative Line of Business (LoB)

Other Cross-Agency Initiative Line of Business (LoB)	Other Cross-Agency Initiative / LoB Description	DoD Mission Area	FEA BRM LOB	FEA BRM LOB Sub-Function
Information Sharing Environment LOB (ISE LOB)	The ISE LOB consists of multiple sharing environments designed to serve five communities of interest (COIs): intelligence, law enforcement, defense, homeland security, and foreign affairs. The ISE will provide a distributed, secure, and trusted environment for transforming terrorism information sharing into actionable information for community-wide sharing.	EIE	Information and Technology Management	Information Sharing
Homeland Security Presidential Directive 12 (HSPD-12)	Presidential directive mandating adoption of a common identification standard (HSPD-12) for all Federal employees and contractors. HSPD-12 has been mandated and implementation plan is currently being executed DoD is working with other agencies on follow-up actions, including participation on interagency boards for technical issues, and on the Federal Identity Credentialing Committee for policy issues.	EIE	Information and Technology Management	Information Systems Security

OMB Assessment Framework and DoD EA Annual Plan

The OMB Assessment Framework, on an annual basis, requests a self-assessment to determine DoD EA completion and use for results and recommends actions that will improve effectiveness of the EA and therefore, improve the effectiveness and efficiency of DoD performance. Due to the visibility of these efforts, it is important to the Department that this assessment accurately reflects DoD's accomplishments as it may have a direct bearing on future budget requests and score on the DoD EA portion of the President's Management Score Card.

The OMB Assessment Framework outlines the specific requirements for an effective Transition Strategy; the DoD EAC Community of Practice (CoP) provides implementation guidance for DoD managers to help them develop their transition and sequencing plans in accordance with the OMB Assessment requirements. Sequencing plans create the historical context from which we can see how well our improved processes influence our programs to meet their targets, provide benefits and accomplish outcomes. Note: the OMB emphasis on documentation and artifacts actually has an adverse effect in that it encourages a proliferation of documents regardless of process effectiveness.

The DoD EAC CoP develops a DoD Annual Plan to address and leverage the recommendations of the OMB Assessment, improve DoD EA processes, and use as a structure to measure progress toward maturity based on OMB guidance. The DoD Annual Plan sets quarterly goals that incrementally address the weaknesses noted in the Assessment. By addressing the weaknesses noted, we abate risk and mange the effectiveness of our programs. The quarterly report of the DoD EA Annual Plan isT reviewed with OMB and adjusted as necessary as goals are realized and other goals and objectives are added. These quarterly reports are also used to satisfy the requirements for EA quarterly reporting for the President's Management Score Card

In addition, the GAO assessment process (EAMMF) includes a periodic review of DoD EA and delivers a maturity model assessment that is designed to help the Department to better address weaknesses in their EA program. The DoD EAC CoP leads the development of a DoD plan to document, prioritize and implement the GAO recommendations in a consistent manner.

The OMB and GAO assessments have defined timelines whereby DoD has responsibility to respond and provide documentation on a quarterly and annual schedule. The DoD EAC CoP is developing a process to identify and consolidate the information and processes required by OMB and GAO and therefore facilitate DoD executive efforts to not only provide this information in a timely manner but to also use it to affect the major decision processes of the department concerning DoD EA.

DoD EA Transition Strategy Process and Annual Update

Future versions of the DoD EA Transition Strategy process will follow a similar methodology to this version, which includes collection of DoD IT300 Exhibits' transition and sequencing plans, an expanded collection of other major and related DoD initiatives and programs, and the compilation and analysis of transition and sequencing plans with related performance measures. Guidance to DoD managers to compile and submit this information will be provided. Also, the results of the analysis will be leveraged for use in the DoD EA RMs where appropriate, particularly in the Performance Reference Model.

In addition, the DoD EA Transition Strategy will continue to align as necessary with other DoD processes, policies, and governance efforts, including the 8000 series policies, the GIG Architectural Vision and the DoD EA Federation Strategy, and to work

with the EDFWG for alignment of strategic statements throughout the DoD and contribute to fill identified gaps.

The DoD EA Transition Strategy will also strive to leverage all internal work to develop common capability definitions and Capability Increments as a critical need for DoD to provide a base for transition planning. The OMB and GAO Assessments will also continue to be leveraged to improve DoD performance thus capturing the value of EA to enhancing mission performance.

The DoD EA CRM provides guidance to DoD executives for identification and documentation of metrics to measure projected and desired outcomes. The Department has documented its performance measurement process as shown in the DoD EA CRM, and analyzed the performance measures from the DoD EA CRM with the performance measures of the IT 300 initiatives as shown in Appendix D, *DoD IT300 Exhibits Investments' Planned Improvements for 2006 to the Actual Results for 2007.* Integration of EA measures with other processes such as the Systems Development Lifecycle (http://akss.dau.mil/dag/) and Information Resources Management (*DoD IRM Plan*) have also occurred. The DoD performance measurement process is documented in the *DoD - Blueprint for Establishing Risk-based Governance of IT investments.* These two documents are posted on core.gov*.*

The Defense Acquisition Guidance states the goal of establishing outcome-based performance measures and that the performance measurement indicators and processes are monitored measured and updated as they progress through the acquisition milestone lifecycle.[12] Further, performance measurement indicators and processes are monitored, measured, and updated on a regular basis; the results of which can be seen in the *DoD Performance and Accountability Report*.

Summary

Service, Agency, and Component Commander strategic visions and architectures are being developed in consonance with, and as extensions to, the GIG Architecture and in accord with their Title 10 responsibilities are supporting DoD mission area managers develop their extensions to the GIG Architecture. The Department's vision, architecture and supporting elements and policies are providing the unifying thread for each Service and Mission Area. Building from a common architectural foundation, the systems that the Services are acquiring will become part of the GIG as they are developed and delivered.

This enterprise architecture work greatly increases our nation's ability to conduct effective, responsive operations. Our capabilities are being strongly enhanced because of major improvements in situational awareness, Joint Force interoperability, reductions in operational cycle times, ability to dynamically and continuously plan operations, ability to perform effects-based operations, and ability to rapidly adapt to battlefield conditions.

[12] Defense Acquisition Guidebook

Section 4. Target Capability View

This section describes the GIG Architectural Vision, the vision for the DoD "target" architecture for the Net-Centric Environment (NCE). This is updated from the GIG Capstone description in the DoD EA Transition Strategy 2007.

Section 4 Contents:

Introduction

A major element of DoD transition planning is the progress toward the target GIG. A summarized version of the *GIG Architectural Vision* will be described in this section of the DoD EA Transition Strategy.

The target GIG vision is for an agile, responsive, and unified GIG that enables the Department to fully leverage the power of information and collaboration across the Enterprise to the forward edge of the battlespace. The GIG Architectural Vision, V.1.0, of June 2007 describes the target GIG in a short, high level, understandable way. This version of the GIG Architectural Vision describes a target GIG that is not static but one that is characterized by its ability to rapidly and effectively incorporate operational, systems, and technical change. Through the development of a series of time-phased GIG Capability Increments, today's GIG will evolve towards the target GIG described in this Vision. The articulation of capability increments and spirals in an evolutionary cycle will combine with the GIG Architectural Vision and other architecture resources, such as the DoD Architecture Registry System (DARS), DoD IT Standards Registry (DISR), DoD IT Portfolio Repository (DITPR), and OMB's Select and Native Programming Data Input System- IT (SNaP-IT), to comprise and document the DoD "target" architecture.

The GIG Architectural Vision is a critical document for DoD executives and managers to use as a high-level target capability view for developing their individual transition strategies. The GIG Architectural Vision e will provide the framework for implementing the overall DoD EA Transition Strategy in an evolutionary manner.

For purposes of describing the target capability view in this document, this section extracts from and summarizes the GIG Architectural Vision v1.0, 27 June 2007, particularly in how it relates to the DoD EA Transition Strategy. The GIG Architectural Vision can also be found at http://www.defenselink.mil/cio-nii/docs/GIGArchVision.pdf

GIG Architectural Vision Introduction

The centerpiece of today's Defense transformation to net-centric operations (NCO) is to become more agile in response to the security challenges of the 21st century. Greater levels of agility are achieved by leveraging the power of information. The GIG Architectural Vision is key to creating the information sharing environment and will be critical to transformation to NCO.

Part of this transformation to the future GIG will be the way the GIG supports the exchange and management of information and services. The future GIG will enable visibility, accessibility, sharing, and understanding of all information and services among all DoD users, as well as mission partners through well-defined interfaces. A key element of the future GIG will be its ability to extend that visibility, accessibility, and sharing to unanticipated users. The future GIG will provide mission assurance; that is, both information sharing and information assurance on trusted, interoperable networks. As a result, the GIG will support and enable highly responsive, agile, adaptable, and information-centric operations characterized by:

- An increased ability to share information
- Greatly expanded sources and forms of information and related expertise to support rapid, collaborative decisionmaking
- Highly flexible, dynamic, and interoperable communications, computing, and information infrastructures that are responsive to rapidly changing operational needs
- Assurance and trust that the right information to accomplish assigned tasks is available when and where needed, that the information is correct, and that the infrastructure is available and protected

Advances in technology and corresponding innovations in operational concepts and operating practices provide improved information capabilities. These improved information capabilities are the foundation for evolving the current GIG to the target GIG – a dynamic, agile, and robust GIG that meets or exceeds the information requirements of the Department by enabling information and decision superiority.

Figure 6 shows all components of the GIG Architecture and the relationship among those components. The DoD Architecture Baseline describes the current DoD environment and the existing GIG capabilities that support operations in today's environment. The DoD Transition Strategy includes an Enterprise-level transition plan built from Mission Area, Joint Capability Area, and DoD Component portfolio transition plans and GIG Capability Increments. The GIG Capability Increments describe future, required operational (warfighting, business, and Defense intelligence) capabilities and the GIG capabilities required to support them. GIG Capability Increments are time-phased as determined by functional owners and GIG capability developers.

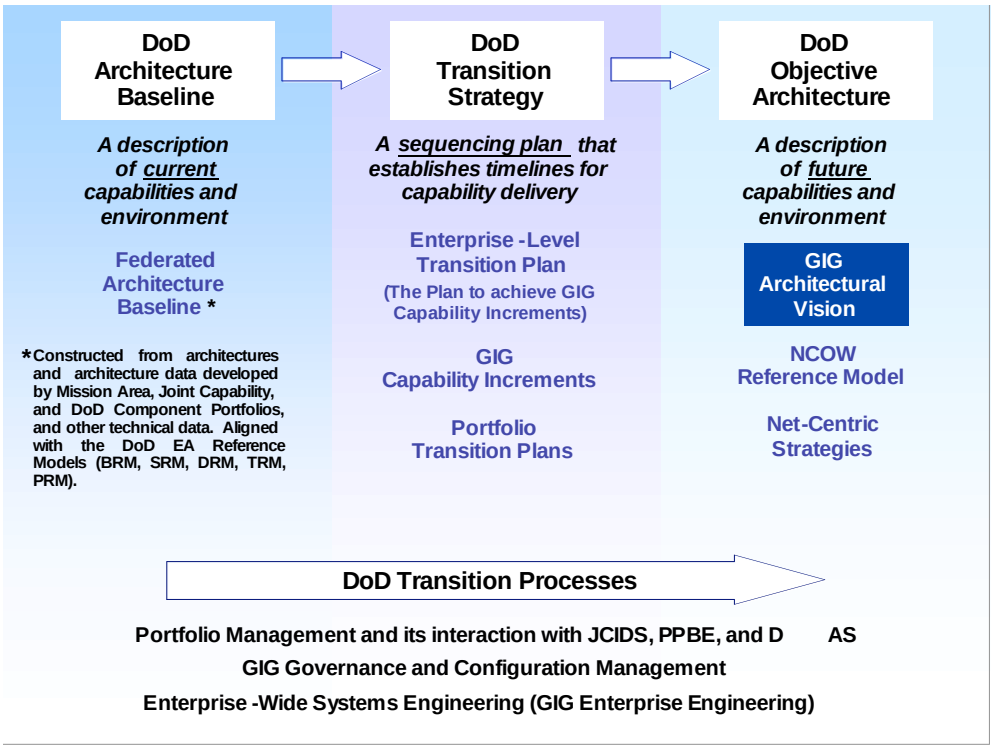


Figure 6 – The GIG Architecture (The DoD Enterprise Architecture)

The GIG Architectural Vision, in combination with other, more detailed descriptions (Net-Centric Operations and Warfare (NCOW) Reference Model and the net-centric strategies), provides the focus for the development of the GIG Capability Increments. **Figure 7** illustrates this concept (with notional dates).

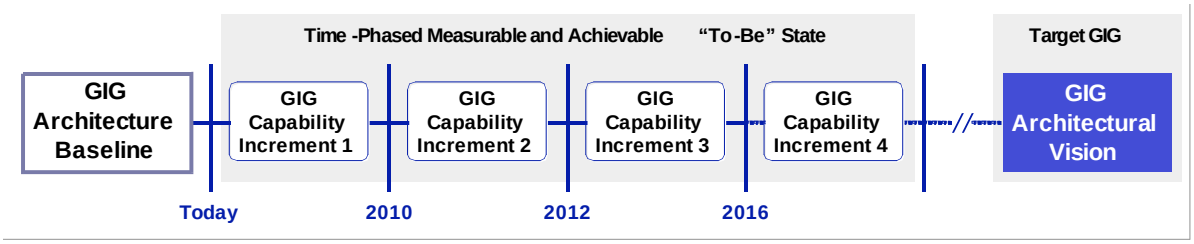


Figure 7 – Transition from GIG Architecture Baseline to GIG Architectural Vision

The GIG Architecture is described through a set of artifacts that document operational activities, information flows, data requirements, services and applications, IT infrastructure, and technical standards.

The GIG Architecture, which is the DoD Enterprise Architecture, is achieved through a federated approach to ensure an integrated, coherent transition to the target GIG through time-phased incremental capabilities. This federated approach applies to the development of architectures at the Department, Mission Area, Component and

Program levels. The GIG Architecture description provides the detailed information needed to both capture the baseline and define the target envisioned in this document.

The GIG Architectural Vision was developed using various DoD documents as its foundation. These documents also serve as the foundation for the DoD EA Transition Strategy. The GIG Architectural Vision complements the GIG Technical Foundation with an integrated overview across the multiple modules of the foundation - from operational to technical.

The Target GIG

Overview of the Target GIG

The target GIG allows all DoD users[13] (and their external mission partners[14]) to find and share the information they need, when they need it, in a form they can understand, use, and act on with confidence; and protects information from those who should not have it. GIG capabilities are effectively aligned to enable a dynamic and responsive end-to-end operational environment, (1) where information is available (2) the means to produce, exchange, and use information are assured and protected; and (3) where resources such as bandwidth, spectrum, and computing power are dynamically allocated based on mission requirements and implemented through the use of precedence, priority and resource allocation techniques.

The Operational Benefits of Achieving the Target GIG

Some examples of the operational benefits this information sharing environment provides include:

- Increased Shared Situational Awareness and Understanding on the battlefield, in business processes, and intelligence operations through near–real-time information sharing and collaboration. Users can relate the information to their particular situations and perspectives; draw common conclusions; make compatible decisions; and take appropriate action related to the overall situation.
- Increased Speed of Command through the real-time availability of quality information for decision making and the ability to rapidly and effectively disseminate direction including the Commander's intent.

[13] DoD users include information providers and (anticipated/unanticipated) information consumers, whether fixed or on the move, deployed or at fixed installation, human or software/hardware.

[14] Mission partners generally participate through a secure gateway. These gateways permit members to be authenticated, produce and consume information services, and collaborate. However, the GIG and associated services also must allow unclassified information to be exchanged with uncleared civil-military partners outside the boundaries of the DoD Enterprise.

- Greater Lethality results from the real-time availability of trusted, reliable information at widely dispersed locations with different classification levels, improved command and control, and enhanced collaboration.
- Greater control of Tempo of Operations by depending on networked environment (and global reach) to support dynamic planning and redirection.
- Increased Survivability through improved situational awareness.
- Streamlined Combat Support by providing users access to the latest, most accurate, most relevant information (e.g., re-supply order status and tracking).
- Effective Self-Synchronization through shared situational awareness, collaboration, and understanding of the Commander's intent.
- Effective Self-Organization of support organizations through shared situational awareness and collaboration, including understanding of the warfighter's changing and present needs.
- Increased Agility & Efficiencies across DoD business operations through interoperability of business systems/applications and establishment of common business services, where appropriate.

Over time, the dramatically improved information capabilities, provided by the target GIG, enable new concepts of operations, new tactics, and new processes/procedures in support of warfighting, business, and Defense intelligence missions and operations.

Operational Vision of the Target GIG

This section examines the target GIG from the operational perspective of the users who can be information consumers, information producers or providers, managers or operators of the GIG.

As shown in **Figure 8**, the target GIG supports a wide variety of DoD human and automated information consumers and providers, as well as their mission partners who access the GIG through secure gateways.

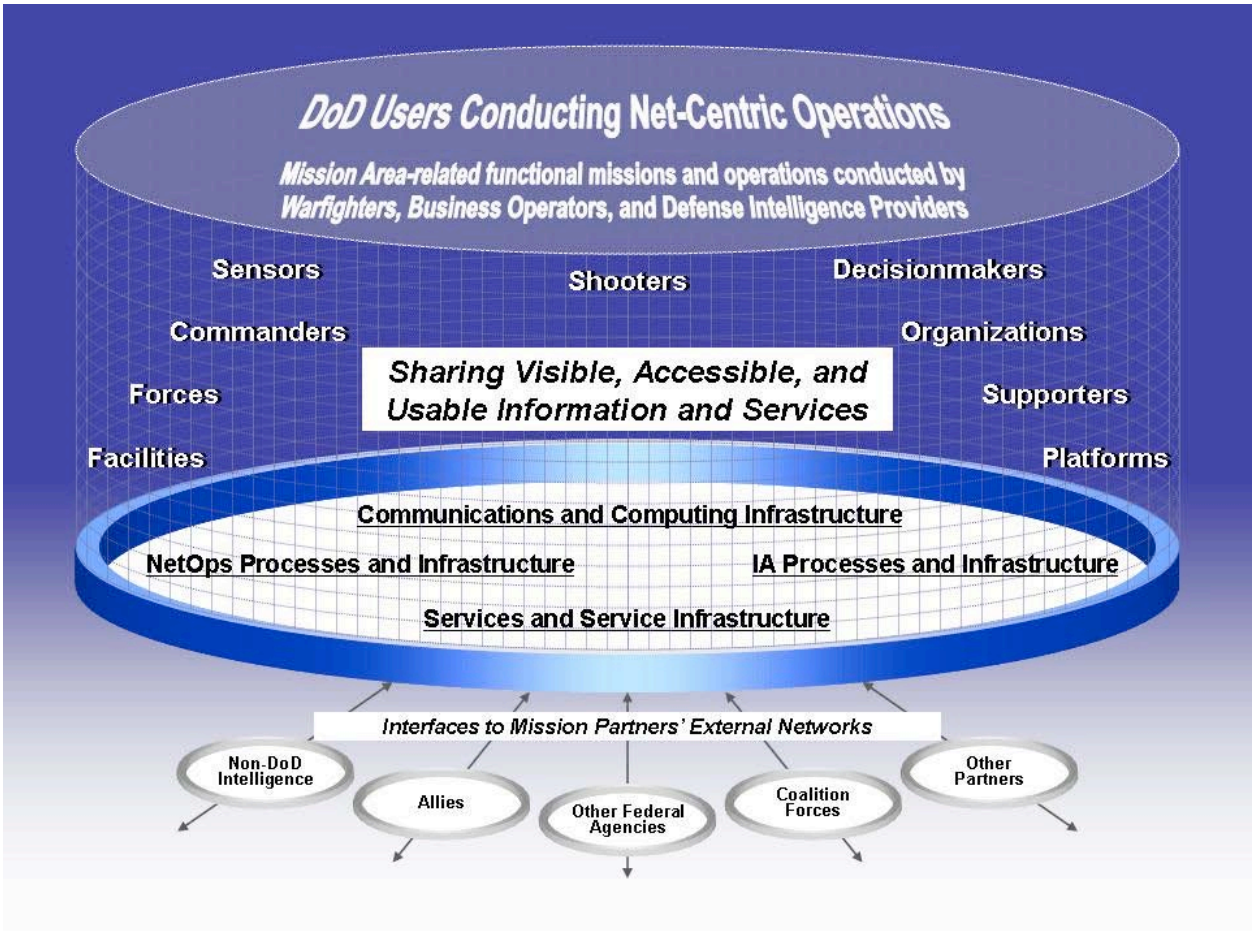


Figure 8 – The GIG and Net-Centric Operations

From a user perspective, access to and use of the target GIG is natural, seamless, persistent, secure and reliable (even under attack) and provides transport, computing and information services at all classification levels.

Figure 9 illustrates information sharing in the target GIG from the perspective of those executing warfighting, business, or intelligence missions. All DoD and Mission Partner GIG users (depicted in the lower part of the figure), with the appropriate authority and trust level, are reliably interconnected to enable them to produce and discover

shareable information and services (depicted in the upper part of the figure). Access to shared information and services are not restricted by chain of command, location, or network limitations.

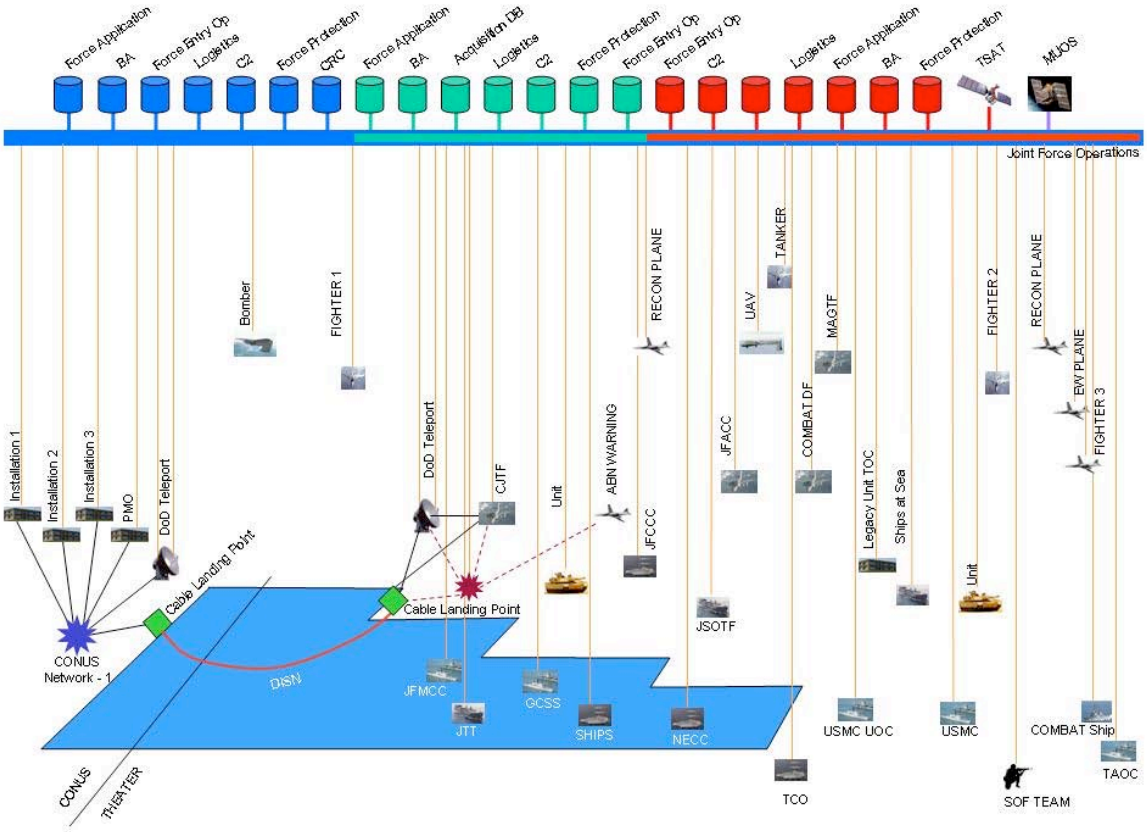


Figure 9 – Information Sharing Within the Target GIG

Information is the key commodity in the target GIG, and vast amounts of data are available in near-real time to information consumers. Sharing information is enhanced through a set of automated activities and capabilities and by the formation of ad hoc Communities of Interest (COIs) focused on sharing information for specific joint missions/tasks. Finally, users explicitly trust the availability, authenticity, confidentiality, non-repudiation, integrity, and survivability of the information, assets, and services of the *assured* target GIG.

Systems Vision of the Target GIG

This section describes the system functionality that enables the information-centric GIG discussed in Section 3. As depicted in **Figure 10,** the systems vision of the target GIG is characterized by two major functional components (infrastructure and the mission-specific applications, services and information) that are operated and defended by NetOps to support user needs.

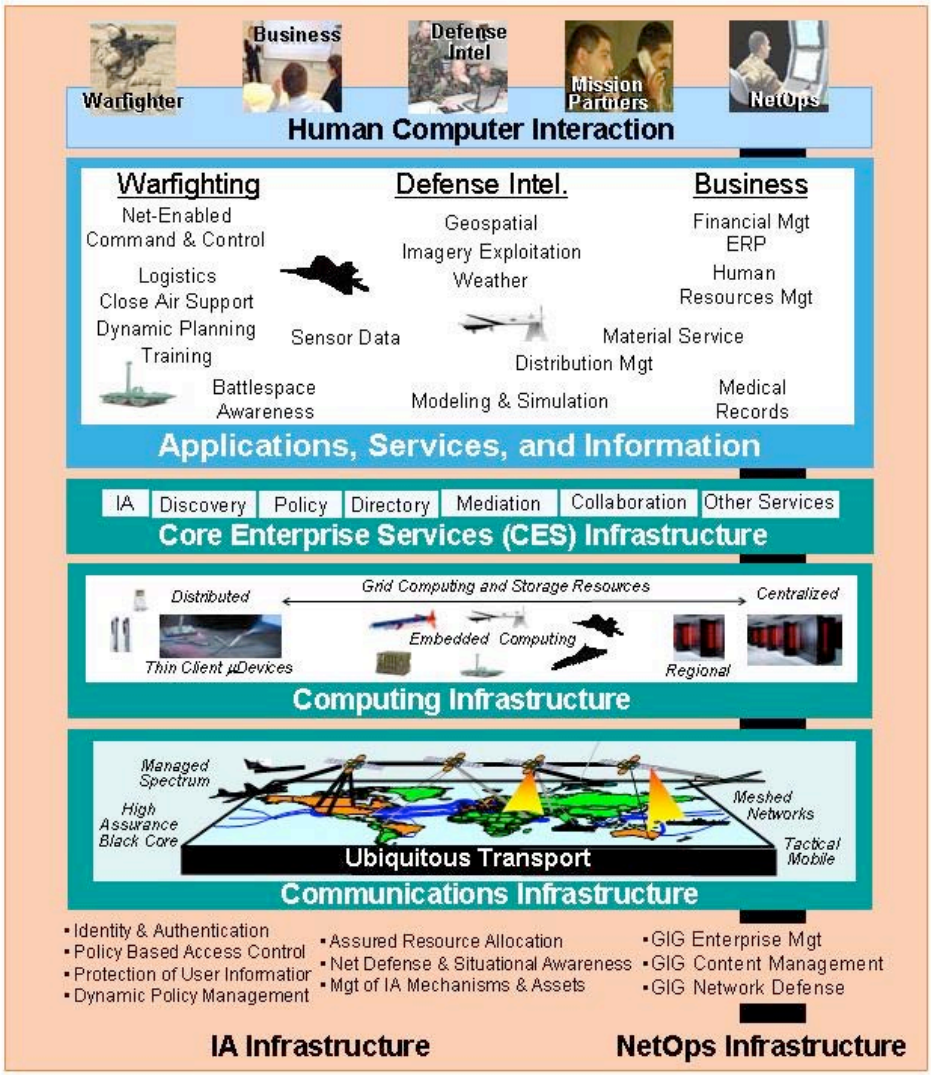


Figure 10 – System Vision of the Target GIG

The heterogeneous GIG infrastructure, globally unified through federation, enables users, including mission partners, to agily transport, store, find, access, process, and secure information across the Department. The communications, computing, Core Enterprise Services (CES), and IA infrastructures of the target GIG are included in the associated domains of the Enterprise Information Environment (EIE) Mission Area (EIEMA) portfolio.

All the major elements of the target GIG in Figure 6 may be reviewed in detail in the GIG Architectural Vision at http://www.defenselink.mil/cio-nii/docs/GIGArchVision.pdf.

The IP-based communications infrastructure is particularly related to the target GIG and is therefore a major element of the DoD EA Transition Strategy. As depicted in **Figure 11**, an IP-based network[15] infrastructure is the foundation of end-to-end interoperability in the target GIG. All types of information such as telephony, multimedia services, video, and data are converged over this universal network.[16]

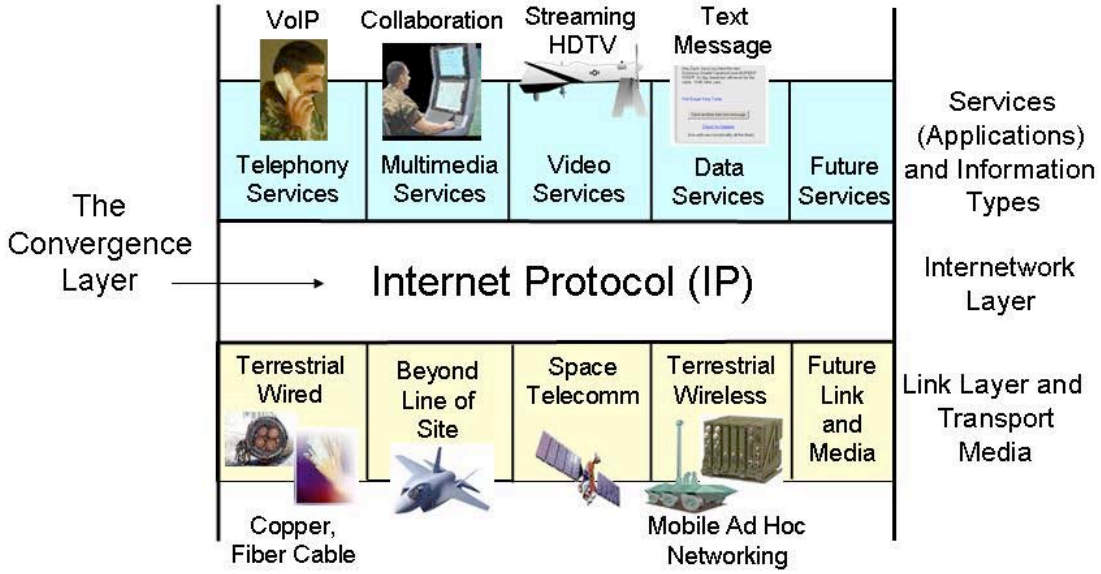


Figure 11 – GIG Internetworking Convergence Layer

Underlying this internetworking convergence layer, all types of DoD-relevant physical transport media and technologies are supported. For instance, this includes copper cable, optic-fiber cable, SATCOM, and tactical wireless (RF and optical). This enables a deployed tactical user to collaborate in real time (without a priori communications planning) with an intelligence analyst in CONUS through mobile ad hoc networks, theater networks, SATCOM, and terrestrial fiber networks (all on a transaction-based, variable trust level).

The IP-based communications infrastructure includes terrestrial, space based, airborne, and wireless segments, instantiated in several key DoD communications programs. **Figure 12** depicts the interconnected nature of these segments in the GIG for DoD users (connections to mission partners are not depicted).

[15] Also referred to as "IPv6 and beyond" to reflect the communications capabilities needed to support the target GIG.

[16] Gateways may still exist between converged IP and tactical environments.

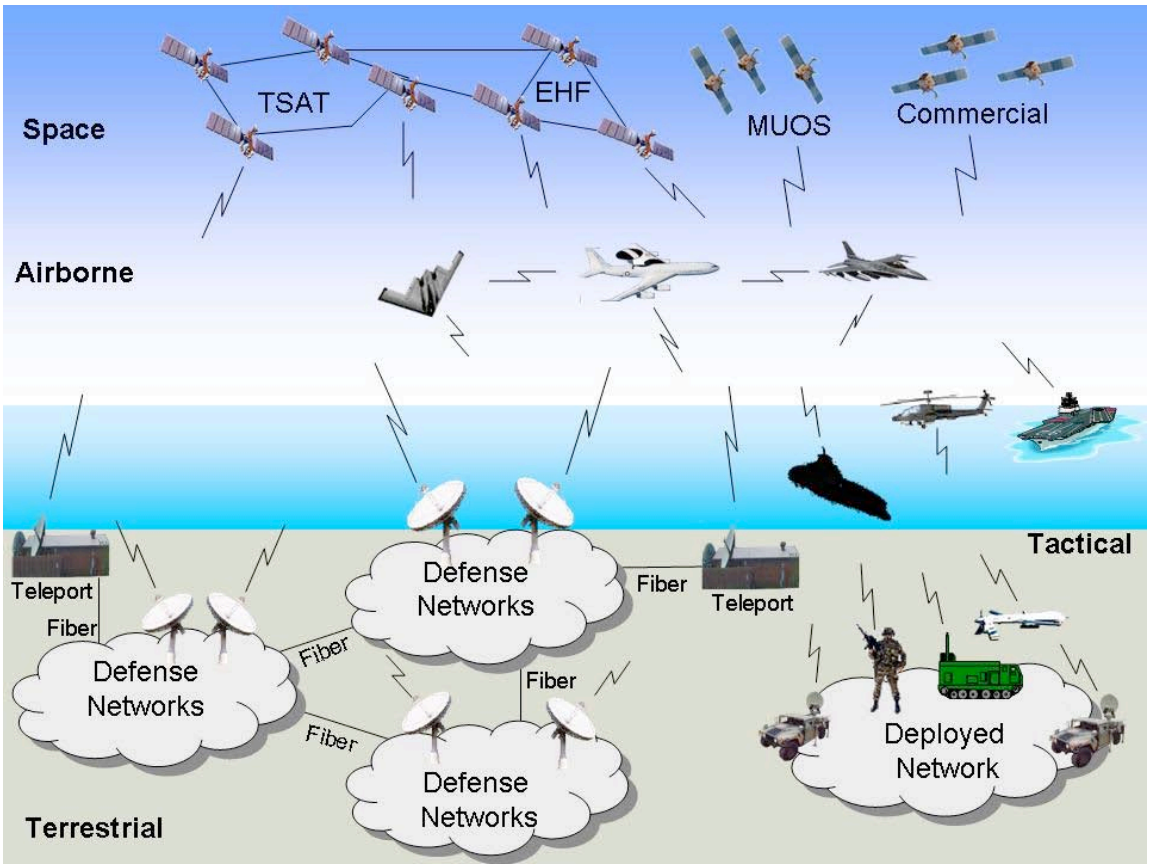


Figure 12 – GIG Communications Infrastructure

Technical Vision of the Target GIG

The technical vision of the target GIG identifies a set of complex technologies[17] that are critical to achieving the system functionality of the target GIG described in the previous section. This section identifies key technologies that enable the functions, systems and services in the target GIG. The relationships among evolving technologies, system solutions, and operational needs are clearly understood and managed in the target GIG.

Key target GIG technologies include:

- IPv6[18] technologies (and beyond) that support an assured, reliable, end-to-end, scalable, and survivable mesh transport infrastructure.
- SOA Infrastructure technologies that provide the tools, capabilities, processes, and methodologies to deploy an SOA-enabled DoD enterprise.
- Mobile Ad-hoc NETworks (MANETs) and sensor technologies that support the building of ubiquitous, assured, and agile tactical networks that are federated with the non-tactical domains of the target GIG. Mobile and sensor technologies enable (1) users, appliances, intelligent agents, and other edge devices, wired or wireless; (2) universal access; and (3) exchange of video, voice, and data information of any kind, from anywhere. These networks are self-healing and allow for reconfiguration around failed nodes.
- Human computer interaction (HCI) technologies that (1) address methodologies, processes, and techniques for designing, implementing, and evaluating human computer interfaces, and (2) provide descriptive and predictive models and theories of interaction. The long-term goal of HCI is to design systems that minimize the barrier between the human's cognitive model of what they want to accomplish and the computer's understanding of the human's task.
- Semantic Web technologies that enable user agents to process and share metadata-tagged, actionable information. This includes the automated metadata tagging and discovery technologies that support information sharing.
- Ubiquitous RFID tagging for tracking of products, components, and humans throughout the target GIG. As with any GIG capability, the extent that tracking of humans is allowed is governed by law and DoD policy.
- Very large scale data storage, delivery, and transmission technologies that support the need to index and retain streaming video and other information coming from the expanding array of theater airborne and other sensor networks. The target GIG supports capacities exceeding exabytes (10^{18} bytes) and possibly yottabytes (10^{24} bytes) of data.
- High performance computing technologies that will enable the full implementation of Grid computing and services.

[17] The target GIG will incorporate these technologies via the associated set of technical, open standards.

[18] IPv6 (Internet Protocol version 6) represents a large set of advanced internetworking capabilities that will mature in the target GIG timeframe. IP will require more advanced mesh technologies to reach the reliability expected in the target GIG.

- Grid computing technologies that provide support and manage an assured federation of heterogeneous computing, storage, and communications assets available from the GIG infrastructure, and managed as Grid Services by NetOps. The physical characteristics of grid services are generally transparent to users and applications. Grid services provide the necessary qualities of service and protection to enhance NCO. Grid services enable the sharing of these assets across DoD administrative, organization, and geographic boundaries.
- Agent technologies provide autonomous support throughout the Net-Centric Environment (e.g., in applications for disconnected users, tactical users, and enterprise management).
- IA technologies that enable transaction-based access control, information sharing across security domains, protection of information and resources, and maintenance of Situational Awareness in the target GIG.
- Black core enabling technologies that support end-to-end protection of information exchanged among users and services located anywhere in the target GIG. The 'core communications infrastructure' of the GIG is the set of diverse networks and connections owned and managed by different DoD services and organizations. A black core is a set of core components where all data traffic moving among these components is encrypted end-to-end. A black core that extends out to the tactical environment to include user networks and devices will support mobility, security, and survivability in the target GIG.[19] Black core enabling technologies will address, for example, scaleable routing, quality of service, and discovery capabilities that will be provided in the target GIG. Black core supports the evolution of the GIG from a system-high perimeter protection model to a transaction-based Enterprise IA protection model. **Figure 13** provides a conceptual view of an end-to-end GIG with a black core.
- Digital Policy Enabling Technologies. In the target GIG, operational activities, system and service functions, and resources such as applications, services, and networks, are governed by automated rules derived from DoD policy. Automated rules are structured as conditions and actions for managing activities and resources in the context of specific realms such as mission areas, domains, cross-domains, and COIs. An example of a current digital policy-based capability is a network management application that dynamically manages IP addresses and QoS at the network level. An example of an emerging digital policy-based technology is Directory Enabled Networking (DEN) which implements policy-based networking to automate the control of large, complex networks.

[19] A. De Simone, J. Tarr, "Defining the GIG Core", draft-gig-defining-the-core-desimone-tarr-051030.pdf, October 2005, www.ietf.org.

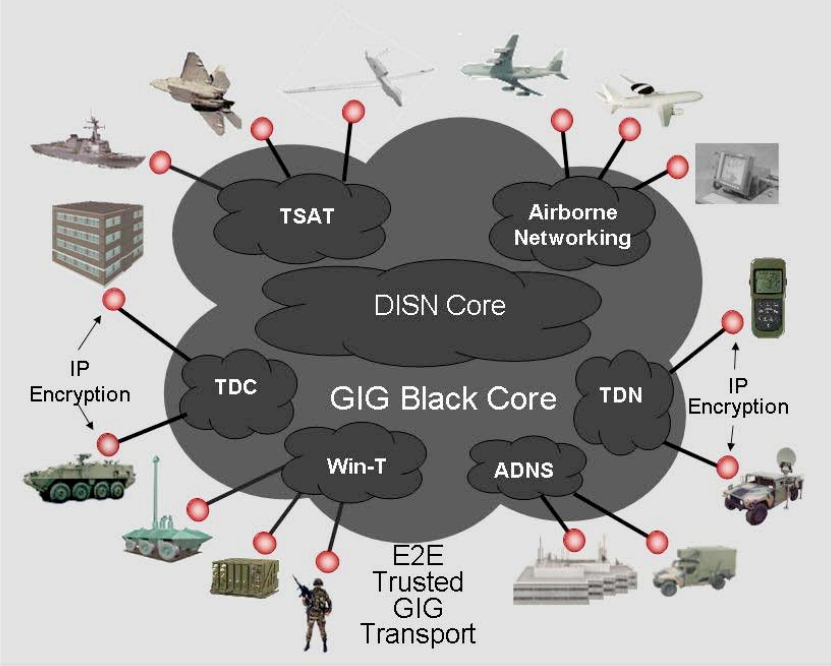


Figure 13 – Conceptual View of an E2E GIG with a Black Core

The complex target technologies identified above contain both sustaining and disruptive components. As the Department has effectively integrated the benefits of disruptive technologies such as the World Wide Web, it will also effectively integrate the benefits of the disruptive components of these target technologies in the future.

Technologies will continue to increase in complexity. Innovations will occur with greater frequency and be adopted in shorter time frames. Continued Department-wide early value determination and adoption of technologies, along with the co-evolution of technologies and operational capabilities, is essential for evolution to the target GIG.

The next section discusses the transformation necessary for achieving the target GIG and beyond.

Achieving the Target GIG

The federated DoD Enterprise Architecture (EA) is a key element in achieving this transition. This approach provides an enterprise-wide common lexicon to support the numerous decisions related to strategy and IT investments needed for success. The federated DoD EA exists as a set of architectures that are linked and aligned via mission, function, and domain taxonomies from the DoD Reference Models (RMs). Individual contents are accessible, visible, and understandable to DoD process decision makers, including those operating and defending the GIG. The DoD EA provides the single source for descriptions of operational processes, GIG Capability Increments, and current and planned IT investments to realize those Increments. It also provides the analytical data source for investment decisions. Enforcement, through architecture governance and existing processes, is the key to success. The vision for architecting the target GIG is a federated architecture approach. **Figure 14** is a notional example of architecture artifact distribution throughout the federated architecture. See **Figure 3** in Current Status, Federation Strategy section for depiction of current DoD Enterprise Architecture.

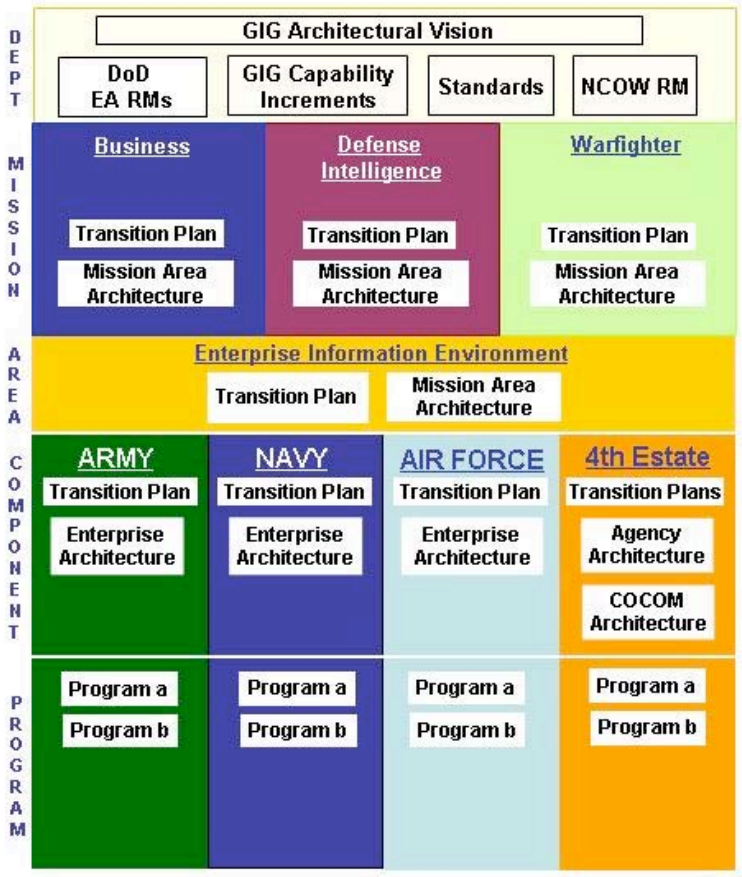


Figure 14 – GIG Federated Architecture Approach (Notional)

This federated architecture approach is described in more detail in the *GIG Architecture Federation Strategy V1.2,* 01 August 2007. This approach provides a framework for enterprise architecture development, maintenance and use that aligns, locates, and links disparate architectures and architecture information via information exchange standards to deliver a seamless outward appearance to users. A Federated Architecture aligns activities, services, systems, and infrastructure with federation standard taxonomies. They also conform to a common context established by rule sets or mappable standards across autonomous Mission Areas, DoD Components, and Programs, thereby minimizing the uniqueness among these autonomous elements.

GIG federation across all DoD Components and with mission partners is critical to achieve a collaborative information sharing capability. This capability must support all phases of conflict, as well as humanitarian assistance and disaster relief. In the target GIG, policies and processes to support this federation – and the ability to dynamically establish appropriate organizational relationships – are in place. Some processes (e.g., Certification and Accreditation, Configuration Management) evolve to better reflect the integrated nature of this target GIG. Information for emerging and existing GIG capabilities will be available and shared through enterprise-wide implementation of the DoD Net-Centric Data Strategy (in concert with the architectural approach just discussed).

Finally, realization of the operational benefits of the target GIG in enabling NCO requires the development and implementation of new concepts of operations, tactics, business processes, and organizational changes for the Department. Training and experimentation are critical in identifying and validating the benefits and risks of information sharing, as well as its impact on NCO.

Section 5. DoD EA Transition Strategy Concept and Components

This section includes the what, why, and how as well as the elements of the DoD EA Transition Strategy.

Section 5 Contents:

- Introduction
- DoD Transition Strategy Components

Introduction

The DoD strategy for migrating from its "baseline" architecture to its next "target" architecture is to create an NCE as described by the GIG Architectural Vision and other related DoD resources and to evolve the NCE as information and information technology management changes.

A graphical description of the "baseline" to the "target" architecture is shown in **Figure 15**.

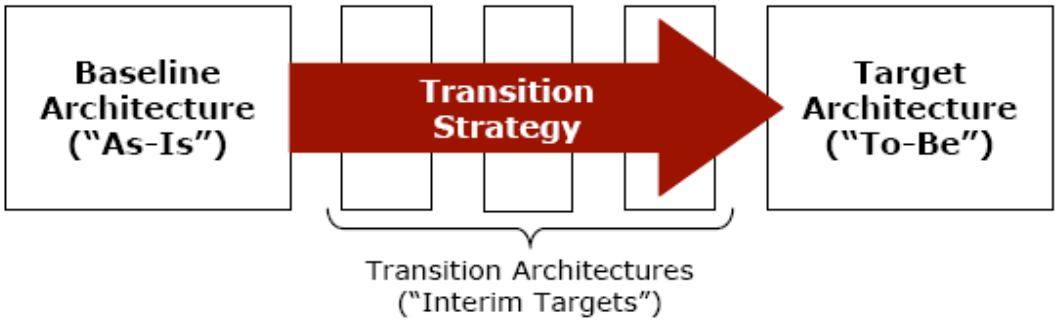


Figure 15 – GIG Architecture v1.0, Transition Architectures (GIG v2.0, net centricity, and SOA) and the "Target" Architecture (as described by the GIG Architectural Vision)

The IT Lifecycle Framework is comprised of three phases – Architecture, Investment, and Implementation – which extend across the entire IT lifecycle. **Figure 16** shows how the DoD EA Transition Strategy fits into the IT Lifecycle Framework.

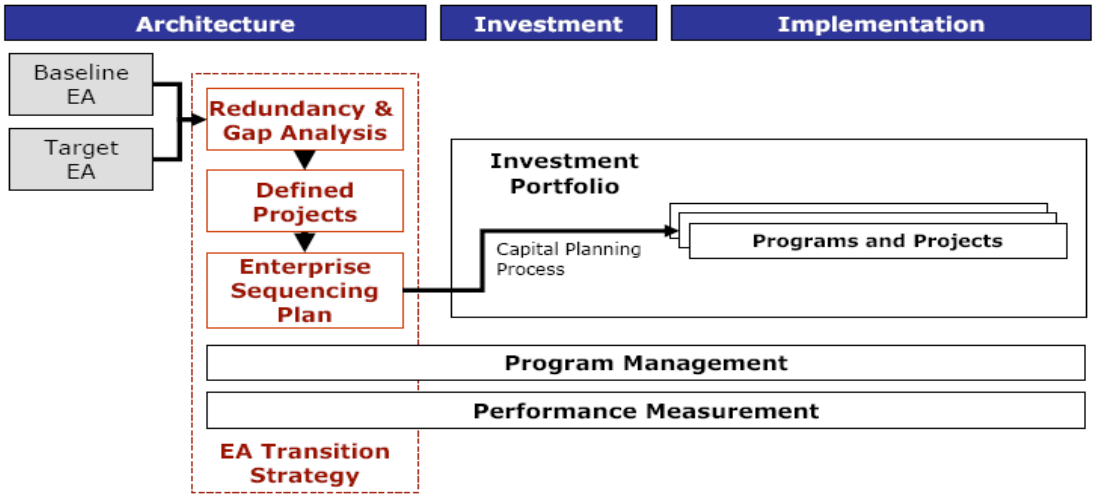


Figure 16 – DoD EA Transition Strategy in the IT Lifecycle Framework

The DoD EA Transition Strategy addresses the multi-year timeframe for which the Department's "target" architecture is defined. The detail and completeness of the GIG Architecture v1.0 was at the level necessary for it to serve as the starting point for this transition strategy. Also, both the "baseline" EA, (GIG Architecture v1.0) and the previous "target" EA (GIG Architecture v2.0) have already been documented in the DoD Architecture Repository (DARS). DARS includes content retrieved from those sources or from Mission Area Architectures as part of the federated GIG Architecture, which is the Department's EA.

As the Department progresses toward its "target" architecture and the GIG Architectural Vision, it will be able to express that "target" in the form of GIG Capability Increments. Periodically, the DoD EA Transition Strategy will be updated to reflect progress through various interim targets toward the "target" described by the GIG Architectural Vision and expressed in Capability Increments.

The DoD EA Transition Strategy is comprised of content extracted from the federated GIG Architecture as described in Section 3 and the GIG Architectural Vision and related Net-Centric artifacts as described in Section 4.

DoD EA Transition Strategy Components

The FEA Practice Guidance and the OMB EA Assessment 2.2 describes the components of an effective EA transition strategy. The DoD Transition Strategy includes links to the following components from the Framework as part of the analysis effort:

- Redundancy and Gap Analysis. The purpose of performing redundancy and gap analysis is to identify opportunities for consolidation or reuse in the "baseline" architecture and to identify gaps between the "baseline" and "target" architectures.
- Defined Programs and Projects. The projects and programs used in the analysis are the major DoD IT 300 Exhibits presented to the White House in the

President's budget. Programs and projects analyzed in this section provide the link between EA and the investment management process. For the purposes of this section, a program is shown at the level of an IT 300 Exhibit. Each show accurate dependencies on produced or consumed Net-Centric capabilities.

- Enterprise Sequencing Plan. The enterprise sequencing plan provides an organization-wide view of programs and projects across the Department at the level of the Department's IT portfolio, as reported in the President's budget, and gives leadership the visibility to use the EA for organization-wide planning. The Enterprise Sequencing Plan analysis enables high-level impact assessment of investment decisions and programmatic changes on the overall plans for moving toward the target decisions and programmatic changes. The effects of those changes on other projects and programs can be identified and dealt with as needed. A conceptual enterprise sequencing plan is shown in **Figure 17**, and the key elements of the sequencing plan are defined below.

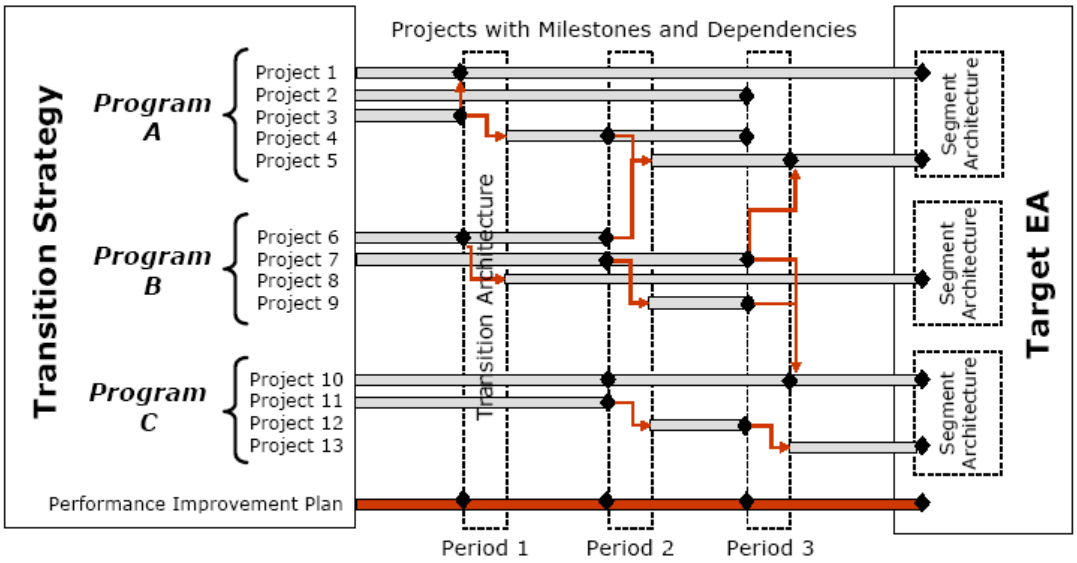


Figure 17 - Conceptual Enterprise Sequencing Plan

- Linkage to the investment portfolio. A primary output from the agency EA Transition Strategy is a proposed IT investment portfolio that can be traced back to a business-approved architectural portfolio. Once projects and programs are architected, agency planners should use these projects as proposed investments to the investment management process (i.e. Select Process). The EA Transition Strategy should include clear linkage between proposed investments and initiatives identified in the business-approved architecture.

- Impact Assessment and Performance. The programs identified in the Transition Strategy should be linked to specific program performance metrics. Coupled with the dependency relationships in the sequencing plan, this provides the ability to assess the performance impact of changes across programs. For example, one program has its budget modified – the dependency between this program and

another program shows the impact this budget adjustment will have on the ability of the second program to meet a planned performance objective.

As the Transition Strategy is updated each year, the success in achieving performance milestones will be assessed against the previous year's plan.

Section 6. DoD EA Transition Strategy Analysis

This section includes an analysis of Mini-Transition Strategies, Net-Centric Maturity Models, and performance information. The 65 DoD Component IT300 initiatives were used as a sample set to represent DoD transition planning.

Section 6 Contents:

Introduction

This section further contains information and analyses that contribute to the content of the DoD EA Transition Strategy as well as meet the criteria for several areas of the OMB EA Assessment. The approach to development of the Strategy sets a methodology in place for future transition strategy development.

For the purpose of this analysis, projects, programs, timelines, and milestones for modernization and transformation activities identified by the DoD IT300 Exhibit investments that serve as a sample set, were collected, compiled, reviewed, and analyzed.

The information was collected by way of the IT300 Exhibit content and the Mini-Transition Strategy input, including the *Net-Centric Maturity Model* (NCMM). Guidance for developing the transition strategies was provided in the *Mini-Transition Strategy Guidance* sent to all the investment managers. The Guidance includes a set of questions that relate to overall transition planning and the level of maturity of net-centric data and services attributes. The set of questions align with criteria in the OMB EA Assessment 2.2 in addition to meeting the criteria recommended for development of a transition strategy in the FEA Practice Guidance. The answers to the questions, in conjunction with IT300 Exhibit input from this sample set, were used as a basis for the analysis of transition planning, net-centric sequencing planning, and performance information and as a foundation for an overall DoD EA Transition Strategy. This compilation of information is the first step in an evolutionary process to develop a transition strategy for an organization as complex and diverse as the Department of Defense.

The individual Mini-Transition Strategies are listed in Appendix B with links to each strategy. The 2008 Army EA Transition Strategy is at Appendix F. The Department of the Navy (DON) Transition Planning document is at Appendix G.

Compiled Answers to DoD EA Transition Strategy Questions

As part of the Mini-Transition Strategy Guidance, a sample set of IT300 Exhibit investments completed a series of questions designed to represent DoD transition planning. Of the total of 65 investments, a total of 54 investments completed the questions; the Army CIO G-6 and the DON also submitted separate papers describing their transition planning from the portfolio perspective. The information was compiled, reviewed and analyzed to excerpt general observations and specific instances to represent a picture of transition status for the sample set of investments. The following describes the type of information collected and an analysis and general observations about the information.

Transition Strategy Overview. *Description of investment's or GIG enabling program's Sequencing Plan in the context of the DoD Baseline Architecture ("As-Is") and the Target Architecture (To-Be") architecture. Use graphics to present the timelines and sequencing plans.*

The overview and enterprise sequencing plans are unique to each investment. All of the investments that responded described their own sequencing plans in the Mini-Transition Strategies. Some of the investments describe their enterprise sequencing plans in terms of a capability roadmap, project plan, or implementation plan. See each Mini-Transition Strategy for details on sequencing plans or equivalent. See Appendix F and G for the 2008 Army and DoN overviews and links.

Status of IT300 Exhibit Investment. *Phase of the acquisition process and/or JCIDS (ICD, CDD, CPD, IOC/Milestone A/B/C, etc.)*

The current milestone/phase is important. Net-Centric Checklist assessments include the status of planning and implementation of data and services attributes and are completed in conjunction with the milestones. The current milestone reflects the level of net-centricity and acquisition documents provide the artifacts for evidence. The analysis shows that the majority of the investments are either at Milestone C or in the deployment or sustainment phase. Several investments are in multiple stages depending on the number of projects within the investment. The length of time the investments have been in the deployment/sustainment phase likely explains why some may not include the same level of net-centric implementation as newer investments.

Location of Artifacts. *Location of your acquisition process artifacts (URL, documents).*

All of the IT300 Exhibit investments have posted their artifacts online. Most of them are available for public access; several require permissions from the investment managers. See the individual Mini-Transition Strategies for locations of their documents.

Joint Capability Areas (JCA). *JCA(s) supported.*

Of the IT300 Exhibits in this sample set, all of the Tier 1 JCAs were represented. Each IT300 Exhibit investment link to the JCAs; therefore the IT300 Exhibit investment links to DoD capabilities and strategic goals. Appendix E, *Chart of DoD IT300 Exhibits Investments' Mission Area, Domain, LOB to DoD Strategic Goals*, further shows the alignment of strategic goals, mission areas, and domains with investments.

Risks. *Effects and impacts the investment or GIG enabling program has on net centricity and adverse impacts on the DoD Net Centric Enterprise if the program or investment is cut, delayed or otherwise not executed according to plan.*

Twelve investments reported a variety of risks if the program were cut or delayed, ranging from loss of support to the warfighter to specific risks to other investments/programs. Some examples include:

- Defense Information System network (DISN): risks to communications transport capability;
- Enterprise Information Decision Support (EIDS) investment: risks to medical and dental readiness and medical surveillance
- Defense Message System (DMS): risk to secure, accountable, and interoperable exchange of information
- Global Combat Support System (GCCS)-COCOM-JTF: risk to continuously available data in a secure environment
- Navy and Marine Corps Intranet (NMCI): risk to Continuity of operations (COOP) and disaster recovery in addition to IT support to Navy and Marine Corps warfighter and business functions
- Public Key Infrastructure (PKI): risk to authenticated and higher assurance credentials for DoD electronic transactions

Dependencies. *Dependencies on Net-centric Enabling Capabilities to accomplish your major outcomes (computing and communications, enterprise services.*

.

As may be expected, Enabling Programs are reported as critical dependencies to many of the other investments. Transport and net-centric services, specifically NCES, were noted most often. Managers of investments need concrete information in regard to timelines and capability increments for implementation of the Enabling Program capabilities in order to set dates for implementing their own capability increments and therefore be able to develop their own accurate transition and sequencing plans. A substantive number of investments have dependencies internal to their program or related programs. Each investment transition strategy in Appendix B includes a section on dependencies where specific dependencies are discussed.

COI Dependencies. *COIs dependent upon for net-centric enabling capabilities and any risks related to these dependencies.*

Most of the respondents to this question indicated similar dependencies as listed in the Dependencies question, many of the COI dependencies are within their own programs or Components. A comment from several investments was that risks related to COI dependencies are associated with ability to apply sufficient resources to maintain COI involvement.

Milestone Alignment. *Milestones are aligned with those of related programs*.

A majority of the respondents indicated that their milestones are aligned with those of related programs. Larger programs reported that they may not know all the dependencies on their program or changes to other programs may be invisible to them.

Performance Improvement./**Achievement of Performance Milestones.** *Cost reduction and performance improvement goals, including interim performance milestones. Milestones were/were not achieved from the previous year's (2006) IT300 Performance Information Table or were completed later than originally scheduled.*

Performance improvement was measured by an analysis of the IT300 Exhibit input in the Performance Information Table for Planned Improvements for 2006 to the Actual Results for 2007. This analysis is presented in the Performance Information Analysis below and in Appendix D.

Additionally, the responses in the Mini-Transition Strategies reflected that most investments did achieve their scheduled performance results. Many of the respondents indicated that they were not required to set performance results for 2007; therefore they were not liable to report results for this cycle.

Note: the analysis of the Mini-Transition Strategies reflects the information received from those investments who responded to the questions. The IT300 Exhibit analysis was directly taken from the Performance Information Table in the IT300. There are differences in the results because of the different sources of the information.

Net-Centric Maturity Model

This analysis was based on the results of the information reported by the investments in the *Net-Centric Maturity Model (NCMM) Analysis*. Guidance to complete the NCMM is in the *Mini-Transition Strategy Guidance*. Appendix C contains two embedded NCMM spreadsheets, one with the data collected from the investments and the other with the compiled results, as well as additional graphics derived from the data.

The NCMM measures the data and services attributes as described in the Net-Centric Data and Services Strategies. Each investment must note the date (year and quarter) of implementation, the level of net-centric maturity based on defined levels provided in the Guidance, and artifacts, such as current phase acquisition documents; net-centric

assessments; planning and program documents; registries; and other similar documentation. Information on the planned use of the DoD Metadata and NCES Services Registries; contact information for Program Managers, Transition Strategy preparers, and Mission Area Managers, are also included in the NCMM. Six of the Army investments completed the NCMM because they completed net-centric assessments in accordance with their acquisition phase.

The analysis of the NCMM shows that most investments have implemented the level of net-centricity necessary for the milestone/phase required by their acquisition process. The planned implementation ties to the unique schedules and requirements of each investment. The level of Net-Centricity achieved is planned to be progressively higher over the next few years with most data and service capabilities coming online between Quarter 4, Fiscal Year (FY) 2007 and Quarter 4, FY 2010. The data and services attributes are roughly on the same schedule per investment. Additional observations include the following:

- A Component with a significant number of programs reported that some of its programs not documented via the IT Exhibit 300 process have achieved a level of Net-Centricity.
- Because the need for net-centric capabilities is recognized, some new programs/investments include a net-centric integration framework to concur with the Net-Centric Data Strategy. For example, the Deployable Joint Command and Control (DJC2) System program was “born Net-Centric” in the midst of evolving Net-Centric requirements.

Figure 18 shows the timeline of net-centric attribute planning/implementation for the sample set. The horizontal bars indicate the quarter and fiscal year of implementation for the net-centric data and services attributes as the investments move from Quarter 4 FY02 through FY12. For more detailed data for the quarter and fiscal year for each investment, see the NCMM Analysis spreadsheet in Appendix C,

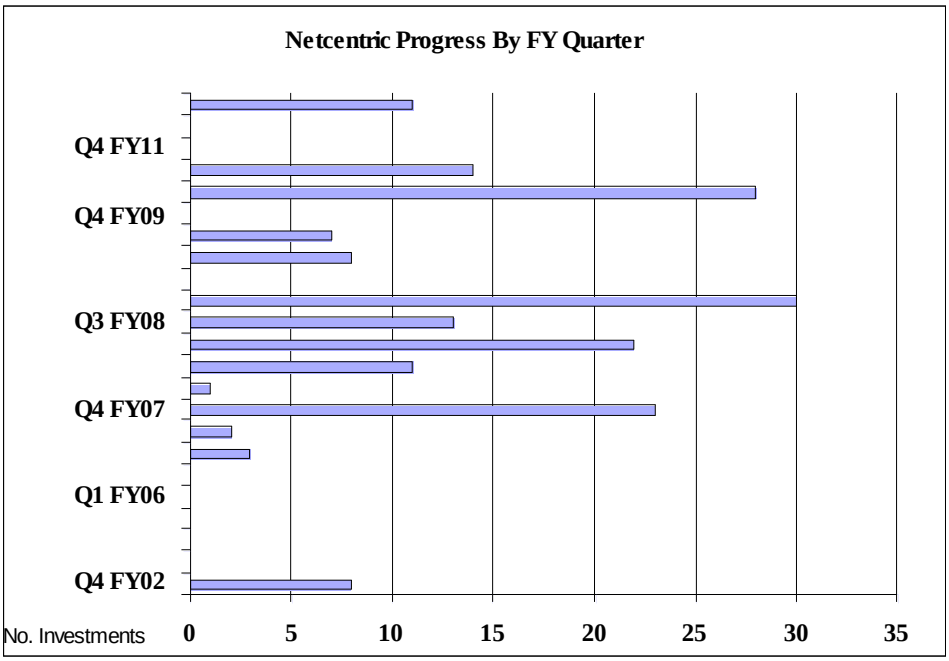


Figure 18 – Net-Centric Progress by FY and Quarter for DoD IT 300 Exhibit Investments

The results provide some insight into the general progress toward the target environment. **Figure 19** shows the levels of net-centricity as of FY07. Of the 60% that responded, approximately 50% are at Level 3. A description of Level 3 follows:

Level 3 – Defined: Structured approach to net-centricity

"To Be" vision is being promoted via policies, procedures, broadening set of DoD compliant standards, and identification of common problems. Re-engineering projects and pilots are being conducted to identify and foster improvements. There are performance metrics for selected programs only. Redundancy reduced data is available centrally with developed and enforced metadata and equally shared management responsibilities. Data has documented structural and semantic meaning such that any potential customer can comprehend and determine how to utilize reliably. Metadata is completely developed. Internal components are mapped to well-defined external interfaces. Unique Web Services built utilizing DoD standards. Estimates of Service usage have been developed. Continuity of Operations Plan has been considered. Offered service dependencies have been determined. Protocols and standards to disseminate service management information considered.

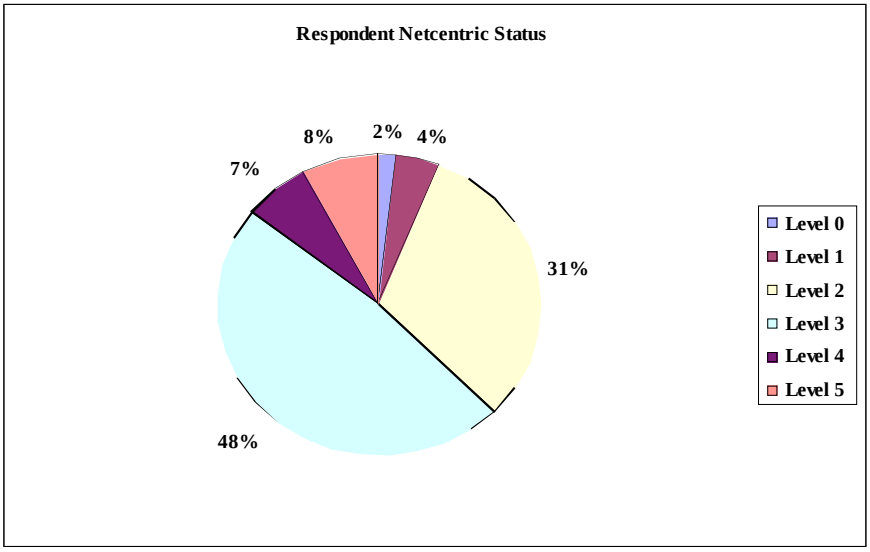


Figure 19 – DoD IT Investments' Net-Centric Status

The results show that there is significant progress from the "as is" to the near term net-centric target as the Department transitions to its target capabilities of 2025. As the target capabilities evolve, attributes to the analysis in future cycles will further detail and clarify the transition to the Net-Centric environment and guide managers in their development of transition plans that will then contribute to refinements of the DoD EA Transition Strategy.

Milestones Consistent with Project Plans. *Milestones for net-centricity in your Transition Strategy/Sequencing Plan consistent with those identified in business cases and project plans for investments.*

Twelve respondents answered yes to this question; sixteen did not answer the question. Analysis is that the investments in the latter group may not document the milestone-to-project plan consistency or that it is inherent in their planning and sequencing plans.

Data Assets. *Data assets in a shared warehouse or other enterprise resource. Shared assets with other COIs.*

The majority of the investments responded Yes on this question, although most data sharing is to internal or external Communities of Interest, including at the Joint and Component-level. In some cases, data is classified and therefore can only be shared with a narrowly-defined set of users.

DoD Metadata Registry and NCES Service Registry. *Detailed plans to register structural metadata in the DoD Metadata Registry and services metadata into the Services Registry.*

The majority of investments plan to register metadata and services when the capability to do so is available, and according to DoD CIO guidance to implement by October 2008. Widespread use of the DoD Metadata Registry may depend primarily on the availability of and knowledge about the mechanics of metadata creation and publishing and the question of how to handle data interdependencies when all investments/programs are not yet entering metadata. The Net-Centric Data and Services Strategies are a necessary and desirable step toward information sharing and reuse.

Internet Protocol v6. *Status, plans, schedules, and implementation of IPv6, and/or dependencies on IPv6 development and implementation by other investments of IPv6 in regard to your investment.*

Most investments have individual IPv6 implementation plans to migrate from IPv4 to IPv6 and/or IPv6 plans are built-in to their program plans. Most investments report a dependence on commercial vendors and some stated the need to await test bed results before migration is possible.

Performance Information Analysis That Supports DoD EA Transition Planning

Appendix D, *DoD IT300 Exhibit Investments' Performance Information Analysis* graphically describes the first two areas of analysis below. Appendix E graphically describes the third analysis.

Alignment of DoD Investments to Performance Measurement Groupings

The data for the first analysis was derived from the IT300 Exhibit Performance Information Table where the 65 investments identified the Measurement Grouping from the FEA CRM as it related to their project. For the purpose of this analysis, only the input for the Technology Measurement Area was reviewed as the assumption was that area would most represent net-centricity. The set of Measurement Groupings that total more than ten in the Technology Measurement Area for all 65 investments are as follows:

- Availability: 42
- Functionality: 36
- Reliability: 23
- Interoperability: 15
- External Data Sharing: 13
- Data Standardization or Tagging: 11
- IT Composition: 10

Of these groupings, only two of the top six Groupings reflect a net-centric attribute: External Data Sharing and Data Standardization or Tagging. The largest grouping, Availability, continues to represent the traditional system (vs. data); for example, how many *systems* are installed at a base and are available to users: 99.9% of *system*

availability. Similarly Functionality is employed to reflect the traditional *system* functionality (vs. service),for example, provide Line of Sight communications.

Analysis of performance outcomes – "Planned Improvements" for 2006 to "Actual Results" for 2007 (from the IT Exhibit 300 Performance Information Table)

For the second analysis, input to the IT300 Performance Information Section was reviewed and analyzed to determine the level of success from the planned improvements that were identified for 2006 to the actual results noted in 2007. Appendix D contains the results of this analysis.

Analysis of Strategic Goals Linked to Investments

Graphical representation of the mapping of the investments to the Mission Areas, Domains, and Strategic Goals (from the Exhibit 300s)

The graphical representations in Appendix E are an example from the Army investments that align the Strategic Goals with the investment by Mission Area and Domains. This information is available from the DoD EA CRM data derived from SNaP-IT. The benefit of this data is to be able to visualize where the investments fall by mission and domain, what major goals are being realized, and therefore be able to see the big picture of DoD investment status.

Summary

The analyses show that the Department has defined programs and projects in support of the NCE, has documented these programs and projects, and has defined the linkage between the strategic goals and objectives and the initiatives in the DoD's FY09 IT Portfolio. The findings from the analysis indicate that there is some degree of Net-Centricity being realized in current IT investments, as represented by 53 of the 65 IT300 Exhibits initiatives; however, there is more work to be accomplished in the collection and analysis of the data. More participation from the IT53 investments in addition to the IT300 investments is needed to better represent net-centric feature of the DoD IT portfolio. Additionally, the information requested from investments for input to the DoD EA Transition Strategy must be tailored to allow for unique investment information as well as to reflect the comprehensive transition planning that Components are developing for their portfolios. Further, the measurement of net-centric maturity via the Mini-Transition Strategies and Net-Centric Maturity Models is based on a sample set. Each investment has unique needs and schedules and therefore there are peaks and valleys in the development process that are not reflected in the compiled data – the prioritization of development of particular attributes is not reflected in the results.

In the case of the NCMM, the uniqueness of each investment's schedule and mission needs must be taken into consideration. For example, this type of assessment of net-centric attributes may not be relevant to the investment or the agency portfolio. The investment may be at the beginning of the acquisition process and has not completed a net-centric assessment. Additionally, some Components may have portfolio planning in

place which is not broken down by individual investment. Net-centric attributes are often embedded in other sets of capabilities and cannot be broken out for the purpose of identifying specifics of timelines and evidence. Net-centric attributes that are embedded in broader capabilities are dependent on other investments to provide infrastructure and so may be difficult to place on an overall timeline.

The essence of the NCMM input, however, was to ascertain whether or not use of or provisioning of net-centric data and service attributes was planned and when; the investments' have provided artifacts to show that this planning and implementation is taking place and is taking place in accordance with the unique needs of each investment.

To summarize the performance analysis, it shows that it is valuable to compare planned improvements to actual results as stated by the IT300 input. The results of the analysis give a clear picture of whether investments need to modify activities to meet their performance goals.

Section 7: DoD EA Transition Strategy Summary

The DoD EA Transition Strategy is a critical component of the DoD Enterprise Architecture as it describes the overall plan to achieve the “To Be” or target architecture. The FEA Practice Guidance and the DoD Practice Guidance for Federated Segment Architecture and Transition Strategy outline the required content for the DoD EA Transition Strategy.

This DoD EA Transition Strategy 2008 follows the outline of the Guidance and is structured and populated to trace the EA from the strategic level of the Quadrennial Defense Review (QDR) 2006 goals to the current status and target description, as well as to include specific sequencing and transition plans for individual IT investments. With this approach, the DoD EA Transition Strategy results in an overall picture of DoD EA and also serves as a view of DoD IT investments’ plans and implementation levels for net-centricity and transformation in general.

Since the release of DoD EA Strategic Plan 2007, much progress has been made in promoting the EA concepts that lead toward the Net-Centric Environment (NCE). The Current Status section describes updates to DoD strategies and policies as well as the evolution of concepts such as capability-based portfolio management and federation. More attention is being focused on performance management – how to identify metrics and how to track planned improvements to actual results for more effective decision-making. The use of the DoD Metadata Registry, the Net-Centric Enterprise Services Registry, the DoD Consolidated Reference Model, Mission Area Segment Architectures, DoD participation in Cross-Agency initiatives, and use of other DoD repositories and processes, facilitates the ability to collaborate and reuse data and services across DoD. The Target Capability View section outlines the GIG Architectural Vision. The Vision describes DoD operational, technical, and systems target environments and the specific actions to be taken to achieve the goals to effectively support the Warfighter in the NCE.

Finally, the transition planning and implementation data from DoD IT investments were compiled and analyzed for the DoD EA Transition Strategy Analysis section and show that DoD progress toward the NCE can be measured and reported as a tool for management. In addition to measuring the level of maturity for data and services attributes in the Net-Centric Maturity Model, the collected and analyzed data also provides a view of the investments' risks and dependencies, alignment with Joint Capability Areas, the status of data sharing and Community of Interest participation, and milestone status, in addition to use of data and services registries.

In summary, the DoD EA Transition Strategy documents the "as-is"(current state) and "to-be" (target state) and samples large IT investments’ progress toward realization of the GIG Architectural Vision capabilities to enhance DoD's overall mission performance. The DoD EA Transition Strategy then becomes a management tool for driving the process of architecting first, investing second and implementing third. The DoD EA

Transition Strategy provides the mechanism to repeat this process and track progress annually. The DoD EA program has made much progress in the last year and continues to improve strategies, policies, and processes to achieve the goals outlined in the QDR 2006 and the GIG Architectural Vision.

References

Note: All documents listed as mandates are available for download from OMB E-Government website on the following pages:
• Legislation: http://www.whitehouse.gov/omb/egov/e-1-legislation.html
• OMB Memoranda: http://www.whitehouse.gov/omb/egov/e-3-memoranda.html
• Federal Enterprise Architecture: http://www.whitehouse.gov/omb/egov/a-1-fea.html
• Federal Transition Framework: http://www.whitehouse.gov/omb/egov/a-2-EAFTF.html

DEPARTMENT OF DEFENSE

ASD/(NII), *GIG Architecture Federation Strategy V1.2*, 01 August 2007.

ASD/(NII) Briefing, *NCOE Gap Methodology Quantitative & Qualitative Analysis Follow-up Brief to PA&E*, 27 July 2006.

AS&C, *Large Data Joint Concept Technology Demonstration (JCTD) Program* briefing, October 2006.

Blueprint for Establishing Risk-based Governance of IT Investments, https://collab.core.gov/CommunityBrowser.aspx?id=7361.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01E, *Joint Capabilities Integration and Development System*, May 11, 2005.

CJCSI 6212.01D, *Interoperability and Supportability of Information Technology and National Security. Systems*, 8 March 2006, https://acc.dau.mil/CommunityBrowser.aspx?id=123981.

CJCSM 3170.01B, *Operation of the Joint Capabilities Integration and Development System*, May 11, 2005.

CJCS Memorandum, *Assignment of Warfighting Mission Area (WMA) Responsibilities to Support Global Information Grid Enterprise Services* (GIG ES), September 8, 2004.

Defense Information Systems Agency (DISA), Joint Interoperability Test Command Fort Huachuca Arizona, Department of Defense (DoD) Internet Protocol Version 6 Generic Test Plan, Version 3, July 2007.
URL:https://www.opengroup.org/gesforum/ipv6/uploads/40/14290/JITC_IPv6_Generic_Test_Plan.pdf

DISA, *DoD Metadata Registry and Clearinghouse*, https://metadata.dod.mil/mdrPortal/appmanager/mdr/mdr.

DISA, *PDM III - Implementing the Net-Centric Data Strategy Progress and Compliance Report*, https://metadata.dod.mil/mdrPortal/appmanager/mdr/mdr.

DISA, PEO-GEA, *DoD Information Sharing Metadata Efforts,* Dr. Glenda Hayes, July 2007.

Deputy Secretary of Defense (DepSecDef) Memorandum, *Information Technology Portfolio Management*, March 22, 2004.

DepSecDef Memorandum, *Capability Portfolio Management Test Case Roles, Responsibilities, Authorities, and Approaches*, September 14, 2006.

Department of Defense (DoD) *Continuous Process Improvement Transformation Guidebook*, 12 May 2006

DoD, *DoD 2007 Enterprise Transition Plan (ETP), Defense Business Transformation Overview*, September 2007.

DoD Chief Information Officer (CIO), *GIG Architectural Vision V1.0,* June 2007.

DoD CIO Information Assurance Strategic Plan, Version 1.1, January 2004.

DoD CIO *Information Sharing Strategy*, 04 May 2007.

DoD CIO Memorandum, *Enterprise Information Environment Mission Area (EIEMA) Domain Owner Designations*, July 14, 2004.

DoD CIO Memorandum, *DoD Net-Centric Data Strategy, May 2003,* http://www.dod.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf.

DoD CIO Memorandum *DOD Net-Centric Data Strategy: Visibility – Tagging and Advertising Data Assets with Discovery Metadata* 24 October 2003
DoD CIO NetOps Strategy, , 14 December 2007.

DoD Directive 5000.1, The Defense Acquisition System, *Defense Acquisition Guidebook*, May 12, 2003, http://akss.dau.mil/dag; *Defense Acquisition Guidebook*, Chapter 7 http://akss.dau.mil/dag/DoD5000.asp?view=functional.

DoD Directive 7045.14, *The Planning, Programming, and Budgeting System* (PPBS), May 22, 1984 (Certified Current as of November 21, 2003).

DoD Directive 8115.01, *Information Technology Portfolio Management*, October 10, 2005.

DoD Directive 8320.2, *Data Sharing in a Net-Centric Department of Defense*, December 2, 2004.

DoD 8320.02-G, *Guidance for Implementing Net-Centric Data Sharing*, April 12, 2006.

DoD Instruction 5000.2, Operation of the Defense Acquisition System, May 12, 2003.

DoD Instruction 7045.7, *Implementation of the Planning, Programming, and Budgeting System* (PPBS), May 23, 1984.

DoD, DoD Enterprise Architecture Reference Model (RM) v.03, May 2004, and v.04, September 2005, http://www.dod.mil/cio-nii/cio/execsummary.shtml.

DoD, *Internet Protocol Version 6 Transition Plan v2.0*, June 2006.

DoD CIO Net-Centric Checklist, https://acc.dau.mil/CommunityBrowser.aspx?id=22203.

DoD CIO, Net-Centric Data Strategy, 09 May 2003.

DoD CIO Net-Centric Enterprise Information Assurance (IA) Strategy Annex to the DoD IA Strategic Plan (Final Draft).

DoD, Net-Centric Enterprise Solutions for Interoperability (NESI), Net-Centric Implementation Framework, V 2.1.0, 12 October 2007 URL: http://nesipublic.spawar.navy.mil/docs/part3/Part3_v2pt1-12Oct07.pdf

DoD CIO Net-Centric GIG Capstone, DRAFT v2.2.1.

DoD CIO Net-Centric Implementation Document (NCID000), *GIG Net-Centric Implementation Document Overview, V1.0*, 11 August 2005.

DoD CIO, *Net-Centric Services Strategy*, 04 May 2007.

DoD CIO *Strategic Plan*, v1.0, 2006, http://www.dod.mil/cio-nii/docs/DoDCIO_Strat_Plan.pdf.

Investment Review Plan, https://collab.core.gov/CommunityBrowser.aspx?id=7281.

Joint Concept of Operations for GIG NetOps, Version 3, 4, August 2006.

Joint Staff, Consolidated JCA, 15 January 2008.

Joint Staff, *Net-Centric Operational Environment Joint Integrating Concept* (NCOE JIC), 31 October 2005, http://www.dod.mil/cio-nii/docs/netcentric_jic.pdf.

GIG Capability Spiral, 12 April 2006.

Technology Readiness Assessment Deskbook, May 2005.

Quadrennial Defense Review (QDR) 2006.

OASIS

Reference Model for Service Oriented Architecture 1.0, 2, August 2006.

FEDERAL

Enterprise Architecture Assessment Framework v2.1 Final, December 2006, http://www.whitehouse.gov/omb/egov/documents/OMB_EA_Assessment_Framework_v21_Final.pdf.

OMB A-11.

OMB A-11, s.300.

FEA Practice Guidance, December 2007.

Federal Transition Framework Usage Guide, Pilot Version, June 2006.

Federal Transition Framework Metamodel Reference, Pilot Version, June 2006.

PUBLIC LAW

Public Law 104-106, Division E, the Clinger-Cohen Act ("The Information Technology Management Reform Act of 1996"), Title 40, United States Code.

APPENDIX A: DoD EA Annual Plan

DoD Annual Plan for OMB Quarterly Assessments (based on OMB Assessment Framework v2.2)

DoD EA Annual Plan
and Quarterly Milesto

APPENDIX B: DoD IT300 Exhibits' Mini-Transition Strategies

0392	CITS	COMBAT INFORMATION TRANSPORT SYSTEM	AIR FORCE
0483	ECSS	EXPEDITIONARY COMBAT SUPPORT SYSTEM	AIR FORCE
0487	DEAMS-AF	DEFENSE ENTERPRISE ACCOUNTING AND MANAGEMENT SYSTEM-AIR FORCE	AIR FORCE
1046	AOC-WS	AIR OPERATIONS CENTER - WEAPON SYSTEM	AIR FORCE
1826	ISPAN	INTEGRATED STRATEGIC PLANNING AND ANALYSIS NETWORK	AIR FORCE
1854	BCS-F	BATTLE CONTROL SYSTEM FIXED	AIR FORCE
1911	TBMCS	THEATER BATTLE MANAGEMENT CORE SYSTEMS	AIR FORCE
5069	GCSS-AF	GLOBAL COMBAT SUPPORT SYSTEM - AIR FORCE	AIR FORCE
6170	AFMSS	AIR FORCE MISSION SUPPORT SYSTEM	AIR FORCE
6170	AFMSS	AIR FORCE MISSION SUPPORT SYSTEM _REVIEW IN POWERPOINT	AIR FORCE
6189	JPALS	JOINT PRECISION APPROACH AND LANDING SYSTEM	AIR FORCE
6191	MEECN	MINIMUM ESSENTIAL EMERGENCY COMMUNICATIONS NETWORK	AIR FORCE
6197	BCS-M	BATTLE CONTROL SYSTEM - MOBILE	AIR FORCE
6320	CMC/TW-AA	CHEYENNE MOUNTAIN COMPLEX/TACTICAL WARNING-ATTACK ASSESSMENT	AIR FORCE
NOTE: ARMY INITIATIVES ARE REPORTED AS A PORTFOLIO IN APPENDIX F, *ARMY EA TRANSITION STRATEGY 2007*. THE INITIATIVES MARKED WITH (N-C) IN THE LIST ARE SEPARATELY DOCUMENTED IN THE NET-CENTRIC MATURITY MODEL IN APPENDIX C.			
0314	GFEBS	GENERAL FUND ENTERPRISE BUSINESS SYSTEM	ARMY
0588	MBCOTM	MOUNTED BATTLE COMMAND ON THE MOVE PROGRAM (N-C)	ARMY
0688	DLS	DISTRIBUTED LEARNING SYSTEM	ARMY
1051	FCS-ACE	FUTURE COMBAT SYSTEM-ADVANCED COLLABORATIVE ENVIRONMENT	ARMY
1125	FBS	FUTURE BUSINESS SYSTEM (N-C)	ARMY
1191	MIRS	US MEPCOM INTEGRATED RESOURCE SYSTEM	ARMY
1631	JNN	JOINT NETWORK NODE NETWORK	ARMY
1935	TC-AIMS II	TRANSPORTATION COORDINATORS' AUTOMATED INFORMATION FOR MOVEMENTS SYSTEM II	ARMY
2166	AFATDS	ADVANCED FIELD ARTILLERY TACTICAL DATA SYSTEM (N-C)	ARMY
2180	I3MP	INSTALLATION INFORMATION INFRASTRUCTURE MODERNIZATION PROGRAM	ARMY
2213	MCS	MANEUVER CONTROL SYSTEM	ARMY
5070	GCSS - A	GLOBAL COMBAT SUPPORT SYSTEM – ARMY (N-C)	ARMY
6185	FBCB2	FORCE XXI BATTLE COMMAND BRIGADE AND BELOW (N-C)	ARMY
6198	WIN-T	WARFIGHTER INFORMATION NETWORK-	ARMY

		TACTICAL (N-C)	
6298	LMP	LOGISTICS MODERNIZATION PROGRAM	ARMY
6491	GCCS-A	GLOBAL COMMAND AND CONTROL SYSTEM - ARMY	ARMY
6963	GUARDNET	GUARDNET XXI, THE ARMY NATIONAL GUARD'S WIDE AREA NETWORK	ARMY
1794	SPS	STANDARD PROCUREMENT SYSTEM	BTA
6312	DTS	DEFENSE TRAVEL SYSTEM	BTA
6521	DIMHRS	DEFENSE INTEGRATED MILITARY HUMAN RESOURCES SYSTEM	BTA
0277	CARTS	COMMISSARY ADVANCED RESALE TRANSACTION SYSTEM	DECA
0555	DEBS	DECA ENTERPRISE BUSINESS SYSTEM	DECA
4035	DEERS	DEFENSE ENROLLMENT ELIGIBILITY REPORTING SYSTEM	DHRA
0536	NECC	NET-ENABLED COMMAND CAPABILITY	DISA
0595	DISN	DEFENSE INFORMATION SYSTEM NETWORK	DISA
0615	DMS	DEFENSE MESSAGE SYSTEM	DISA
0881	GCCS-J	GLOBAL COMMAND AND CONTROL SYSTEM-JOINT	DISA
0882	GCSS	GLOBAL COMBAT SUPPORT SYSTEM-COCOM-JTF	DISA
6456	PKI	PUBLIC KEY INFRASTRUCTURE	DISA
6462	TELEPORT	DOD TELEPORT	DISA
6965	NCES	NET CENTRIC ENTERPRISE SERVICES	DISA
5090	BSM	DLA BUSINESS SYSTEMS MODERNIZATION	DLA
0594	DISS	DEFENSE INFORMATION SYSTEM FOR SECURITY	DSS
0342	JTRS C5	JOINT TACTICAL RADIO SYSTEM - CLUSTER 5	JPEO JTRS
6190	JTRS-CLUSTER 1	JOINT TACTICAL RADIO SYSTEM - CLUSTER 1	JPEO JTRS
6524	AMF JTRS	AIRBORNE AND MARITIME/FIXED STATION JOINT TACTICAL RADIO SYSTEM	JPEO JTRS
6587	JTRS(JPO)	JOINT TACTICAL RADIO SYSTEM (JOINT PROGRAM OFFICE)	JPEO JTRS
NOTE: NAVY INITIATIVES ARE ALSO REPORTED AS A PORTFOLIO IN APPENDIX G, *DON NAVY TRANSITION PLANNING.*			
0155	GCSS- USMC	GLOBAL COMBAT SUPPORT SYSTEM - MARINE CORPS	NAVY
0186	NAVY ERP	NAVY ENTERPRISE RESOURCE PLANNING (ERP) AND APPENDIX AND TABLE OF QUESTIONS	NAVY
6046	GCCS-M	GLOBAL COMMAND AND CONTROL SYSTEM - MARITIME	NAVY
6310	NMCI	NAVY MARINE CORPS INTRANET (NMCI)	NAVY
6555	DJC2	DEPLOYABLE JOINT COMMAND AND CONTROL	NAVY
6946	CAC2	COMBINED AIR COMMAND AND CONTROL	NAVY
1030	KMI	KEY MANAGEMENT INFRASTRUCTURE	NSA
0332	MCPR	MILITARY COMPUTER-BASED PATIENT RECORD (INCLUDES #0435 AND 0049)	TMA

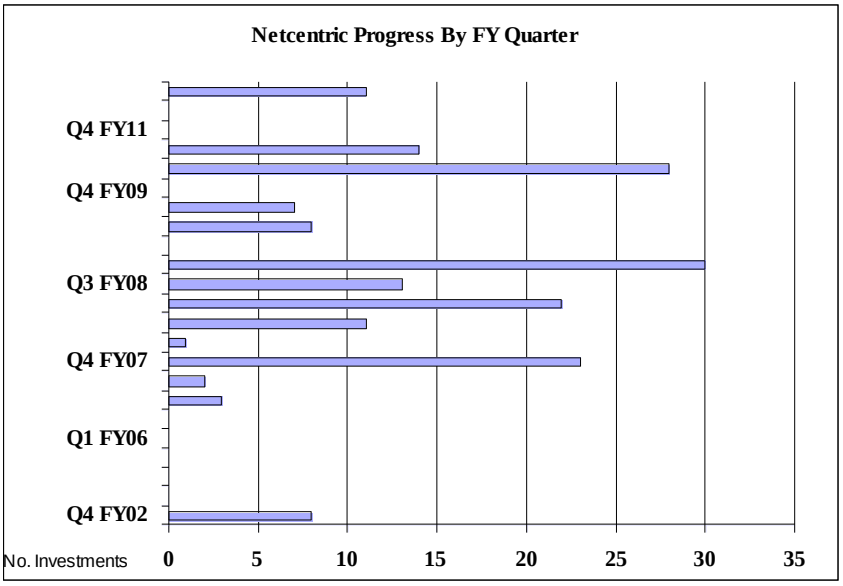
0510	EI/DS	EXECUTIVE INFORMATION/DECISION SUPPORT	TMA
0611	DMHRSI	DEFENSE MEDICAL HUMAN RESOURCE SYSTEM INTERNET	TMA
0613	DMLSS	DEFENSE MEDICAL LOGISTICS STANDARD SUPPORT	TMA
1913	TMIP	THEATER MEDICAL INFORMATION PROGRAM	TMA
0178	DEAMS	DEFENSE ENTERPRISE ACCOUNTING AND MANAGEMENT SYSTEM	TRANSCOM
0884	GDSS	GLOBAL DECISION SUPPORT SYSTEM	TRANSCOM
0884	GDSS	GLOBAL DECISION SUPPORT SYSTEM (TABLE)	TRANSCOM
0884	GDSS	GLOBAL DECISION SUPPORT SYSTEM (PPT)	TRANSCOM
1667	IGC	INTEGRATED DATA ENVIRONMENT/GLOBAL TRANSPORTATION NETWORK CONVERGENCE	TRANSCOM

APPENDIX C. DoD IT300 Exhibits Investments' Net-Centric Capabilities per Net-Centric Maturity Model:

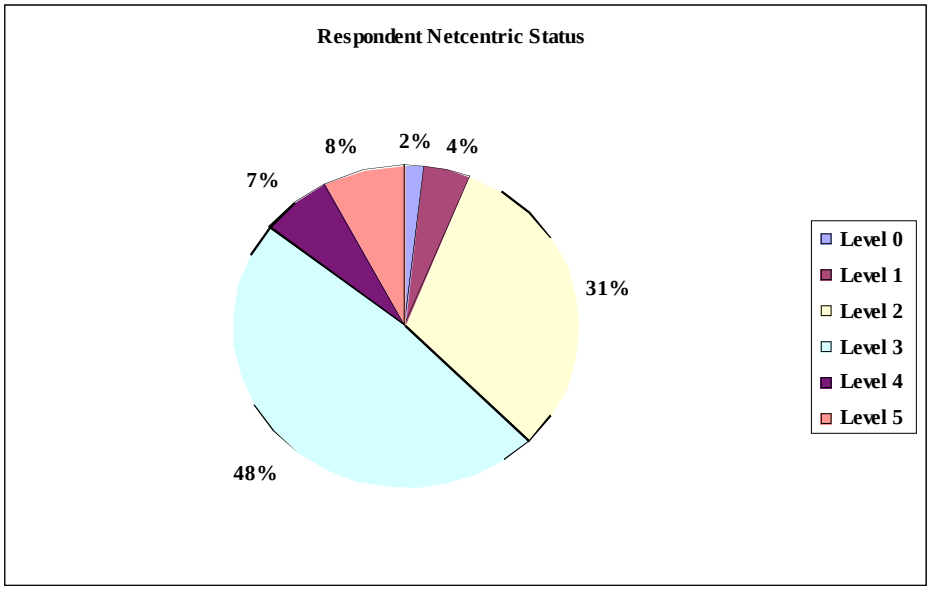
Net-Centric Maturity Model (NCMM) Embedded Spreadsheet with Raw Data and Compiled Results.

NCMM Analysis Spreadsheet	NCMM Data from IT300 Exhibits	NCMM Maturity Levels

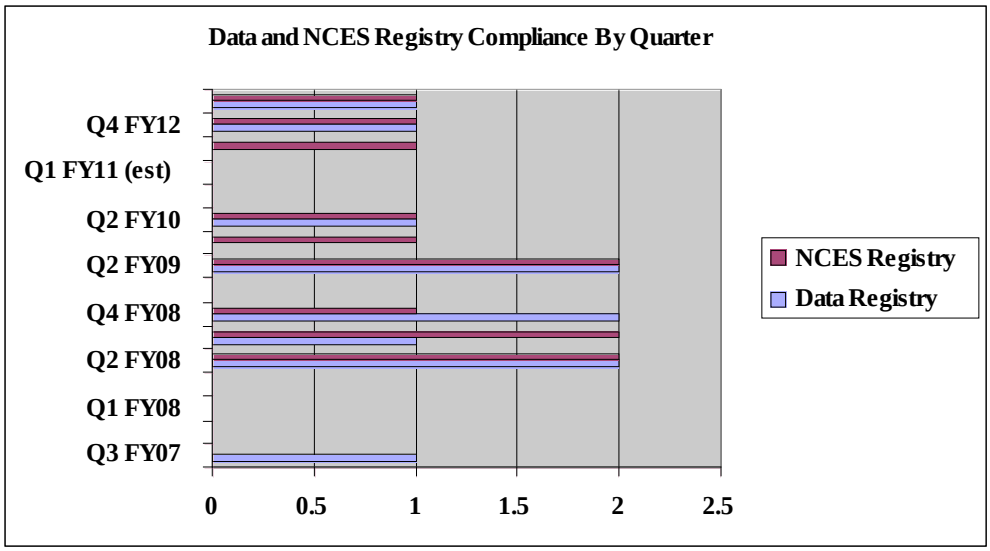
The following graphics shows the timeline and level of net-centricity reported by the IT investments in the NCMM:



Net-Centric Progress by FY and Quarter shows that the majority of Net-Centric progress will occur from Q2 FY08 through Q2 FY10.



Respondent Net-Centric Status shows that of the IT investment respondents (54) that responded, approximately 50% are at Level 3.

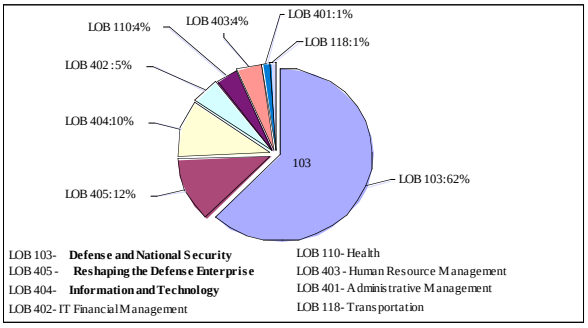


The DoD Metadata Registry and NCES Registry Compliance by Quarter shows use of registries is consistent with projected overall net-centric progress by FY quarter.

APPENDIX D: DoD IT300 Exhibit Investments' Performance Information Analysis

Some Salient PRM Results

Technology Area: (8) Lines of Business; 33 inits



Technology Measurement Groupings:

Availability (42)	Interoperability (15)
Functionality (36)	External Data Sharing (13)
Reliability (23)	IT Composition (10)
Data Standardization or Tagg ing (11)	

2006 - 2007 Technology Observations

- Entries: 53; 15% TBDs or N/As
- Quantifiable Improvements: 35 (66 % of Total)
- Changed Indicators: 18; with improvement: 11.5
- TBDs , N/As, or Indeterminate Progress: 8
- *Distinguishing Phenomena* – 14 MA Changes

2006 - 2007 Planned vs. Actual PRM Results

Processes/Activities Observations

- Entries: 61; 54% TBDs or N/As
- Quantifiable Improvements: 19 (31% of Total)
- Changed Indicators: 15; with improvement: 6
- TBDs , N/As, or Indeterminate Progress: 33

Mission/Business Observations

- Entries: 53; 28% TBDs or N/As
- Quantifiable Improvements: 30 (57% of Total)
- Changed Indicators: 28; with improvement: 17
- TBDs , N/As, or Indeterminate Progress: 15

Customer Results Observations

- Entries: 67; 21% TBDs or N/As
- Quantifiable Improvements: 38 (57% of Total)
- Changed Indicators: 42; with improvement: 22.5
- TBDs , N/As, or Indeterminate Progress: 14

Note: Click here to enlarge the graphic.

This paper reports the salient results from an analysis of the DoD Exhibit 300 Performance Information Table, specifically the comparison between Planned Improvements for 2006 projected by DoD investments in the prior cycle (BY08) and the Actual Results reported in 2007 in the current cycle (BY09). The results are depicted for all four Measurement Areas – Technology, Processes and Activities, Mission and Business, and Customer Results. There are three salient results for the Technology Measurement Area and one set of results for the remaining Measurement Areas. Technology details are enhanced (on the left side of the figure) because the focus of this iteration of the DoD Transition Strategy analysis is information technology (IT)..

With respect to the Technology Measurement Area, the three sets of results are depicted on the left side of the figure to reflect lines of business, measurement groupings, and FY2006-FY 2007 planned improvements versus actual performance results. For the current DoD EA Consolidated Reference Model (DoD EA CRM)

entries, the Technology Measurement Area has 33 initiatives that address eight lines of business (LOB) with LOB 103 Defense and National Security representing the most addressed line of business. There are seven dominant (with 10 or more entries) Technology Measurement Groupings with Availability and Functionality topping the list and nearly tripling their counterparts in every instance. Note that only two of the seven most dominant groupings reflect net-centric attributes and have the lowest number of entries. The largest grouping, Availability, continues to represent traditional system (vs. data) – example, how many *systems* are installed at a base and is available to users. Similarly functionality is employed to reflect the traditional *system* functionality (vs. NCES service) – example, provide LOS communications. The planned versus actual performance results will be explained subsequently but note the distinguishing phenomena for the Technology MA; specifically, Technology was the only of the four Measurement Areas to experience Measurement Area changes (14) from FY2006 to FY2007.

The Planned Improvements versus Actual Results for the remaining Measurement Areas also are recorded (on the right side of the figure). Each Measurement Areas observation contains recordings with the following headings:

- *Entries* are the number of line items in the DoD EA CRM/SNaP-IT database for the FY2006
- *Quantifiable Improvements* reflects the number of all measurement indicators (including changed measurement indicators) that exhibited quantifiable improvements.
- *Changed Indicators* captures two numbers: one, the number of changed measurement indicators; two, the number of changed indicators that exhibited quantifiable improvements either before or after they were changed.
- TBDs, N/As, or Indeterminate Progress' are the number of results that were reported as 'To Be Determined', left blank, or with non-quantifiable progress descriptions

Sample interpretation of Processes/Activities Observations is:

- 54% of the measurement indicators showed no progress during the FY2006-FY2007 interim
- 31% demonstrated quantifiable improvements during the FY2006-FY2007 interim
- 25% of measurement indicators were changed during the FY2006-FY2007 interim where only 40% of the changes can be attributed to successful outcomes in FY2006 (the remaining changes could be attributed to the fact that 2006 were unattainable and therefore changed to improve success ratio during the next interim).

APPENDIX E: Chart of DoD IT300 Exhibits Investments' Mission Area, Domain, LOB to DoD Strategic Goals

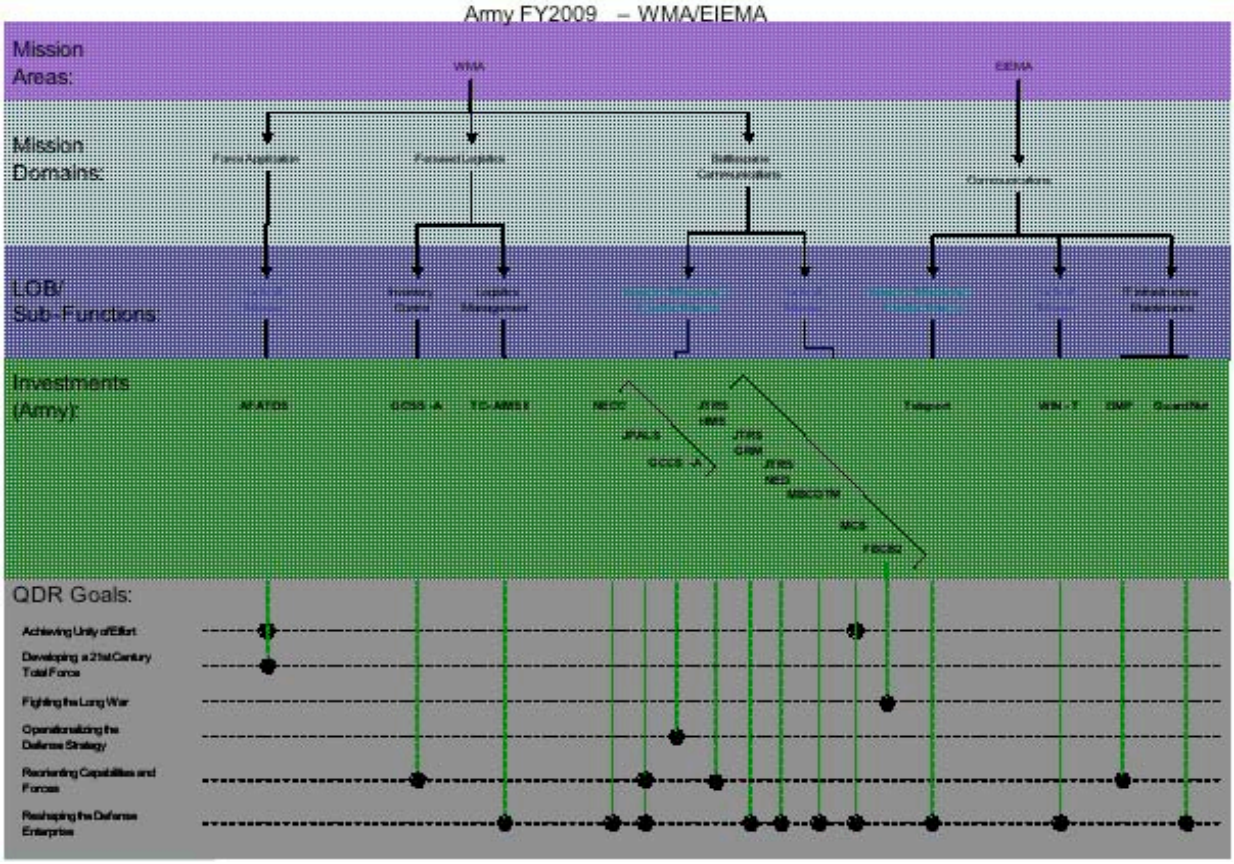


Figure 20. Example using Army Warfighter and Enterprise Information Environment (EIE) Mission Area investments.

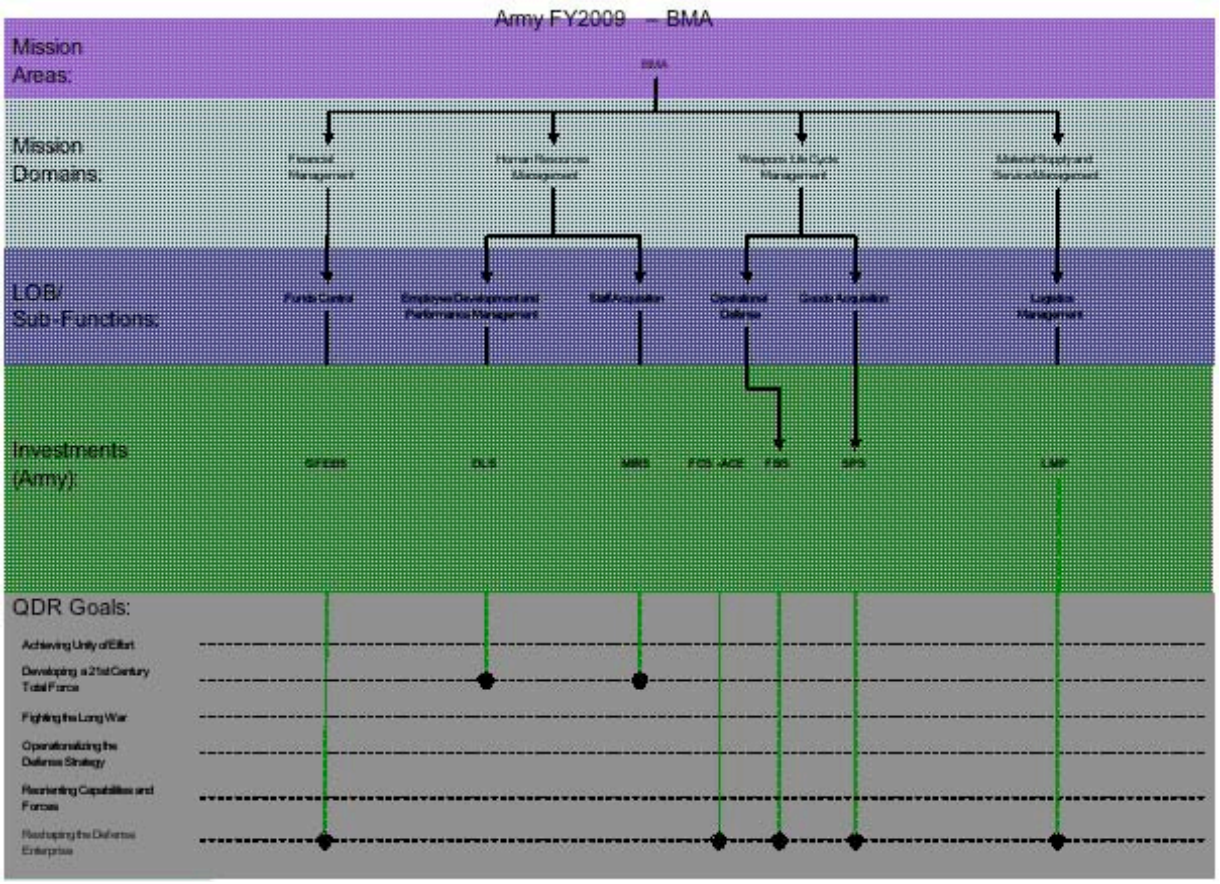


Figure 21. Example using Army Business Mission Area investments.

APPENDIX F: Army EA 2008 Mini-Transition Strategy

2008 Army
Mini-Transition Strate

The embedded document, the *Army 2008 EA Mini-Transition Strategy*, discusses the Army's emerging approach to Enterprise Architecture and key elements of its target architecture.

APPENDIX G: Navy EA Transition Planning

Navy Transition Planning

The embedded document, the *Navy Transition Plan* describes the DON approach to a federated EA that supports the Naval Transformation Roadmap.

APPENDIX H: Business Mission Area Segment Architecture Overview

The Business Mission Area (BMA) Segment Architecture Overview provides summary-level answers to selected questions for the segment per the FEA Practice Guidance. The overview describes the scope, change drivers, vision, performance goals and funding strategy for the segment. The embedded document was submitted by the Business Transformation Agency as part of the BMA Segment Architecture development.

BMA Segment Overview

APPENDIX I: Defense Information Enterprise Segment Architecture Overview

The Defense Information Environment (DIE) Segment Architecture Overview provides summary-level answers to selected questions for the segment per the FEA Practice Guidance. The overview describes the scope, change drivers, vision, performance goals and funding strategy for the segment. The embedded document was submitted as part of the DIE Segment Architecture development.

DIE Segment Overview	DIEA v1.0

APPENDIX J: Warfighting Mission Area Segment Architecture Overview

The Warfighting Mission Area (WMA) Segment Architecture Overview provides summary-level answers to selected questions for the segment per the FEA Practice Guidance. The overview describes the scope, change drivers, vision, performance goals and funding strategy for the segment. The embedded document was submitted as part of the WMA Segment Architecture development.

WMA Segment Overview